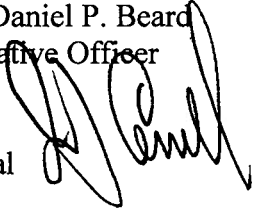


Office of Inspector General  
U.S. House of Representatives  
Washington, DC 20515-9990

MEMORANDUM

TO: The Honorable Daniel P. Beard  
Chief Administrative Officer

FROM: James J. Cornell  
Inspector General 

DATE: August 13, 2007

SUBJECT: Final Report - Audit Of The Financial Statements For The Fiscal Year Ended  
September 30, 2006 (Report No. 07-HOC-08)

The attached report presents the results of the audit of the U.S. House of Representatives' (House) annual financial statements for the fiscal year ended September 30, 2006. Once again, the House received an "unqualified opinion" on its financial statements. An "unqualified opinion" is the best rating given by auditors to financial statements. It means the auditors did not find any financially material discrepancies and found nothing to suggest the amounts on the financial statements were misstated. The Office of Inspector General contracted with Cotton & Company LLP, Certified Public Accountants, to perform the audit. We have highlighted the results of the audit in the attached executive summary.

The results of the audit were discussed with the Chief Administrative Officer (CAO) throughout the audit, and the CAO concurred with all of the reported internal control weaknesses and recommendations for corrective action. The CAO's response is included in the Management Comments section of the report on page 71.

If you have any questions or require additional information regarding this report, please call me at (202) 226-1250.

Attachments



# *Financial Statements*

## *Audit Report*

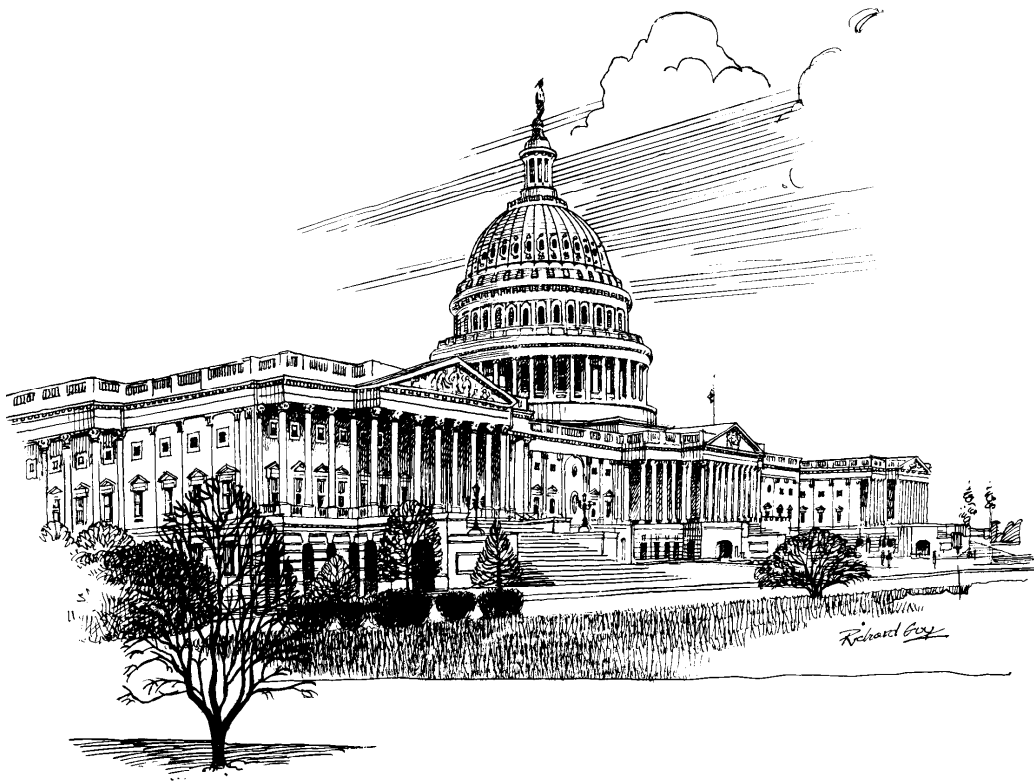
---

---

### *Audit Of The Financial Statements For The Year Ended September 30, 2006*

*Report No. 07-HOC-08*

*August 13, 2007*



# Table of Contents

<b>Executive Summary .....</b>	<b>1</b>
<b>Independent Auditor's Report .....</b>	<b>1</b>
<b>Financial Statements .....</b>	<b>5</b>
Statement of Financial Position .....	6
Statement of Operations .....	7
Statement of Cash Flows .....	8
<b>Notes to the Financial Statements .....</b>	<b>9</b>
<b>Supplemental Financial Schedules .....</b>	<b>23</b>
<b>Independent Auditor's Report on Compliance with Laws and Regulations ....</b>	<b>37</b>
<b>Independent Auditor's Report on Internal Control .....</b>	<b>41</b>
<b>Management Comments .....</b>	<b>71</b>
Management Report on Internal Control	
CAO Response to the 2006 Financial Statement Audit Report	

This Page Intentionally Left Blank



# **Independent Auditor's Report**

This Page Intentionally Left Blank



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

## INDEPENDENT AUDITOR'S REPORT

To the Inspector General  
U.S. House of Representatives

Cotton & Company LLP has audited the accompanying Consolidated Statement of Financial Position of the U.S. House of Representatives (House) as of September 30, 2006, and 2005, and the related Consolidated Statements of Operations and Cash Flows for the years then ended. These financial statements are the responsibility of the Members and administrative management of the House. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial statement audits contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing accounting principles used and significant estimates made by management as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the House as of September 30, 2006, and 2005, and the results of its operations and cash flows for the years then ended, in conformity with accounting principles generally accepted in the United States of America.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The supplemental schedules, Consolidating Statements of Financial Position, Operations, and Cash Flows, are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements. The supplemental schedules have been subjected to the auditing procedures applied in the audit of the basic consolidated financial statements and, in our opinion is fairly stated in all material respects in relation to the basic consolidated financial statements taken as a whole.

In accordance with *Government Auditing Standards*, we have also issued reports dated April 30, 2007, on our consideration of the House's internal control over financial reporting and our tests of its compliance with applicable laws, rules, and regulations. Our reports on internal control and compliance are an integral part of an audit conducted in accordance with *Government Auditing Standards* and, in considering the results of the audits, should be read together with this report.

COTTON & COMPANY LLP

A handwritten signature in dark ink, appearing to read "Matthew H. Johnson".

Matthew H. Johnson, CPA  
Partner

April 30, 2007  
Alexandria, Virginia

This Page Intentionally Left Blank

# Financial Statements

**U.S. House of Representatives**  
**Consolidated Statement of Financial Position**  
**as of September 30, 2006 and September 30, 2005**

	<u>2006</u> <u>Consolidated</u>	<u>2005</u> <u>Consolidated</u>
<b>ASSETS</b>		
Fund Balance with U.S. Treasury (Note 4)	\$ 174,705,449	\$ 212,013,832
Cash (Note 4)	1,673	120
Fund Balance with U.S. Treasury and Cash	<u>174,707,122</u>	<u>212,013,952</u>
Accounts Receivable, Net (Note 5)	745,799	1,141,708
Advances and Prepayments (Note 6)	2,707,359	4,055,971
Inventory	1,883,757	1,325,633
Property and Equipment, Net (Note 7)	<u>48,844,205</u>	<u>54,584,235</u>
Total Assets	<u>\$ 228,888,242</u>	<u>\$ 273,121,499</u>
<b>LIABILITIES AND NET POSITION</b>		
Accounts Payable (Note 9)	\$ 31,686,613	\$ 25,356,370
Capital Lease Liabilities (Note 8)	1,188,252	1,258,747
Accrued Funded Payroll and Benefits (Note 10)	8,057,874	7,755,802
Accrued Unfunded Annual Leave and Workers' Compensation (Note 10)	10,542,142	9,405,463
Deferred Credits (Note 11)	720,599	903,087
Unfunded Workers' Compensation Actuarial Liability (Note 12)	19,610,394	18,537,652
Other Liabilities	<u>414,878</u>	<u>374,858</u>
Total Liabilities	<u>72,220,752</u>	<u>63,591,979</u>
Unexpended Appropriations	121,516,521	166,493,777
Cumulative Results of Operations	<u>35,150,969</u>	<u>43,035,743</u>
Total Net Position (Note 13)	<u>156,667,490</u>	<u>209,529,520</u>
Total Liabilities and Net Position	<u>\$ 228,888,242</u>	<u>\$ 273,121,499</u>

**U.S. House of Representatives**  
**Consolidated Statement of Operations**  
**for the Years Ended September 30, 2006 and September 30, 2005**

	<u>2006</u> <u>Consolidated</u>	<u>2005</u> <u>Consolidated</u>
<b>REVENUE AND FINANCING SOURCES</b>		
Revenue from Operations		
Sales of Goods	\$ 2,817,117	\$ 2,984,305
Sales of Services to Federal Agencies	4,772,769	6,151,926
Sales of Services to the Public	1,025,913	745,167
Interoffice Sales (Note 14)	0	0
Other Revenue	662,440	574,296
Total Revenue from Operations	<u>9,278,239</u>	<u>10,455,694</u>
Financing Sources		
Appropriations to Cover Expenses:		
Appropriations Received (Note 15)	1,251,428,239	1,178,153,355
Appropriations Yet To Be Received (Note 15)	4,055,919	4,071,204
Imputed Financing Source (Note 16)	57,557,337	53,898,845
Total Revenue and Financing Sources	<u>\$ 1,322,319,734</u>	<u>\$ 1,246,579,098</u>
<b>EXPENSES</b>		
Personnel Compensation	\$ 697,824,676	\$ 672,385,410
Benefits (Note 16)	293,609,713	277,737,350
Postage and Delivery	33,964,506	16,772,839
Repairs and Maintenance	53,346,715	53,112,983
Depreciation and Amortization (Note 7)	20,924,290	21,637,129
Rent, Utilities, and Communications	26,465,487	25,726,780
Telecommunications	27,302,317	27,283,288
Supplies and Materials	15,368,008	16,635,462
Travel and Transportation	36,490,909	33,538,007
Contract, Consulting, and Other Services	67,369,517	71,697,077
Printing and Reproduction	28,508,206	12,800,156
Subscriptions and Publications	12,118,166	7,484,729
Cost of Goods Sold	6,235,174	8,462,940
Other Expenses	511,993	165,925
Bad Debts	367,810	40,499
Interest on Capital Leases	230,927	242,928
Total Expenses	<u>\$ 1,320,638,414</u>	<u>\$ 1,245,723,502</u>
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	<u>\$ 1,681,320</u>	<u>\$ 855,596</u>
<b>CHANGE IN NET POSITION</b>		
Net Position, Beginning Balance	\$ 209,529,520	\$ 198,779,660
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	1,681,320	855,596
Plus (Minus) Non-Operating Changes	(54,543,350)	9,894,264
Net Position, Ending Balance	<u>\$ 156,667,490</u>	<u>\$ 209,529,520</u>

**U.S. House of Representatives**  
**Consolidated Statement of Cash Flows**  
**for the Years Ended September 30, 2006 and September 30, 2005**

	<b>2006</b> <b>Consolidated</b>	<b>2005</b> <b>Consolidated</b>
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>		
Excess/(Deficiency) of Revenue and Financing Sources over Expenses	\$ 1,681,320	\$ 855,596
Adjustments affecting Cash Flow		
Appropriations Affecting Cash	(1,149,082,842)	(1,077,719,070)
(Increase)/Decrease in Accounts and Interoffice Receivable	395,909	(881,314)
(Increase)/Decrease in Advances and Prepayments	1,348,612	4,401,067
(Increase)/Decrease in Inventory	(558,124)	32,946
Increase/(Decrease) in Accounts and Interoffice Payable	6,330,243	1,352,751
Increase/(Decrease) in Other Accrued Liabilities	2,369,025	(357,013)
(Gain)/Loss on Disposal of Assets	494,493	165,925
Depreciation and Amortization	20,924,290	21,637,129
Net Cash Provided/(Used) by Operating Activities	<u>(1,116,097,074)</u>	<u>(1,050,511,983)</u>
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>		
Purchase of Property and Equipment	<u>(14,575,436)</u>	<u>(16,162,781)</u>
Net Cash Provided/(Used) by Investing Activities	<u>(14,575,436)</u>	<u>(16,162,781)</u>
<b>CASH FLOWS FROM FINANCING ACTIVITIES</b>		
Appropriations	1,101,125,520	1,090,048,193
Funds Returned to the U.S. Treasury	(7,689,345)	(7,753,623)
Principal Payment on Capital Lease Liabilities	<u>(70,495)</u>	<u>(58,492)</u>
Net Cash Provided/(Used) by Financing Activities	<u>1,093,365,680</u>	<u>1,082,236,078</u>
Net Cash Provided/(Used) by Operating, Investing, and Financing Activities	(37,306,830)	15,561,314
Fund Balance with U.S. Treasury and Cash, Beginning	<u>212,013,952</u>	<u>196,452,638</u>
Fund Balance with U.S. Treasury and Cash, Ending	<u>\$ 174,707,122</u>	<u>\$ 212,013,952</u>



## **Notes to the Financial Statements**

## NOTE 1 - DESCRIPTION OF THE REPORTING ENTITY

The U.S. House of Representatives (House) is one of two separate legislative chambers that comprise the Congress of the United States. The other is the U.S. Senate (Senate). All lawmaking powers of the Federal government are given to the Congress under Article I of the Constitution of the United States. The House and Senate jointly agree on a budget for the Legislative Branch and submit it to the President of the United States. The Members of the House serve two-year terms of office, which coincide with the sequential numbering of the entire Congress.

To help carry out its constitutional duties, the House creates committees of Members and assigns them responsibility for gathering information, identifying policy problems, proposing solutions, and reporting bills to the full chamber for consideration. The House appoints unelected officers to administer both legislative and non-legislative functions, which support the institution and its Members in carrying out its legislative duties. The consolidated comparative financial statements of the House provide financial information on the activities of all entities, which are subject to the authority vested in the House by the U.S. Constitution, public laws, and rules and regulations adopted by the membership of the House.

These financial statements reflect the organizational structure of the House under the 109<sup>th</sup> Congress. The following is a summary of the entity groupings as they appear in the fiscal year 2006 consolidating financial statements:

House **Members** are elected from congressional districts of approximately equal population. The financial information aggregates transactions of the Member districts and Washington, D.C. offices, and includes 435 Representatives; four Delegates, one each, from the District of Columbia, Guam, Virgin Islands, and American Samoa; and one Resident Commissioner from Puerto Rico.

The **Committees** financial information aggregates transactions of the Standing and Special and Select Committees of the 109<sup>th</sup> Congress. Committees are organized at the beginning of each Congress according to their jurisdictional boundaries incorporated in the Rules of the House. The Committees of the House under the 109<sup>th</sup> Congress are:

- Committee on Agriculture
- Committee on Appropriations
- Committee on Armed Services
- Committee on the Budget
- Committee on Education and the Workforce
- Committee on Energy and Commerce

- Committee on Financial Services
- Committee on Government Reform
- Committee on Homeland Security
- Committee on House Administration
- Committee on International Relations
- Committee to Investigate the Preparation for and Response to Hurricane Katrina
- Committee on the Judiciary
- Committee on Resources
- Committee on Rules
- Committee on Science
- Committee on Small Business
- Committee on Standards of Official Conduct
- Committee on Transportation and Infrastructure
- Committee on Veterans' Affairs
- Committee on Ways and Means
- Permanent Select Committee on Intelligence

The House **Leadership Offices** financial information aggregates transactions of:

- Speaker of the House
- Majority and Minority Leaders
- Majority and Minority Whips
- Party Steering Committees, Caucus or Conference, which consist of Representatives of the same political party

The **Officers and Legislative Offices** financial information aggregates transactions of all legislative support and administrative functions provided to Members, Committees, and Leadership offices, including:

- Chaplain
- Chief Administrative Officer
- Office of Emergency Planning, Preparedness and Operations
- Clerk of the House
- Office of the General Counsel
- Office of Inspector General
- Office of the Historian
- Office of the Law Revision Counsel
- Office of the Legislative Counsel
- Parliamentarian
- Sergeant at Arms

The **Joint Functions** financial information aggregates transactions of the joint activities of the House and the Senate to the extent that the House funds these functions in whole or in part. House administrative management does

not exert direct control over the expenditures of these functions. The joint functions in these statements include:

Attending Physician  
Joint Committee on Taxation, which has members  
from both the House and the Senate

**Eliminations** on the consolidating financial statements are used to negate the effect of financial transactions between House entities. Consolidated House financial information would be misleading if inter-entity transactions were not eliminated.

## NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

### A. Basis of Consolidation

The financial statements include the accounts and significant activities of the House. The consolidated financial statements do not include legislative agencies that support the House and that receive separate appropriations. These agencies are:

Library of Congress  
Congressional Budget Office  
Government Accountability Office  
Government Printing Office  
U.S. Botanic Garden  
Architect of the Capitol  
U.S. Capitol Police

Functions jointly shared between the House and the Senate are included in the consolidating financial statements to the extent their operations are funded by House appropriations. These consist of:

Attending Physician  
Joint Committee on Taxation, which has  
members from both the House and the Senate

All significant interoffice balances and transactions have been eliminated to arrive at consolidated financial information.

### B. Basis of Accounting

The House, in accordance with generally accepted accounting principles, utilizes the accrual basis of accounting, which provides for the recognition of events as they occur, as opposed to when cash is received or disbursed. Therefore, revenues are recorded when earned and expenses are recorded when a liability is incurred, without regard to receipt or payment of cash. The accrual basis of accounting contributes significantly to the development of accurate cost information needed to report the financial position and results of operations.

Effective fiscal year 2006, the House changed its financial statement reporting from calendar year (January-December) to fiscal year reporting, (October 1, 2005 to September 30,

2006). The 2005 amounts in the comparative statements are different from the published amount for calendar year 2005 due to the fiscal year conversion.

### C. Fund Balance with the U.S. Treasury and Cash

Funds available to the House to pay current liabilities and finance authorized purchases are held with the U.S. Treasury.

- Fund Balance with the U.S. Treasury includes House accounts, as well as the Congressional Use of Foreign Currency account, which is held at the U.S. Treasury and is maintained and administered by the Department of State on behalf of the House.
- For purposes of the Consolidated Statement of Cash Flows, funds held with the U.S. Treasury are considered cash.

### D. Accounts Receivable

Accounts receivable consists of money owed the House by Federal agencies, Members, employees and/or vendors less an Allowance for Doubtful Accounts.

### E. Advances and Prepayments

Advances consist of payments to Federal government entities for contractual services and for mailings that require address corrections or additional postage. Prepayments primarily consist of prepaid subscriptions for publications and data communication services.

### F. Inventory

The *Gift Shop* and the *Supply Store* maintain an inventory of goods for sale. These entities are included with Officers and Legislative Offices in the consolidating financial statements. Inventories for sale are valued at the moving weighted average method.

The *Furniture Support Services*, also included with Officers and Legislative Offices, maintains inventories of such items as hardwood, carpet, leather, fabric, furniture components, and repair materials. These items are not for

sale and are reflected in the financial statements at an estimated value based on the first in/first out inventory valuation method.

#### **G. Property and Equipment**

Property and equipment including computer purchases are capitalized if the unit acquisition cost is equal to or greater than \$25,000 and the item has a useful life greater than one year. Software is capitalized if the unit acquisition cost is equal to or greater than \$10,000 and the item has a useful life greater than one year. The costs of such items are recognized as assets when acquired. An appropriate portion of an asset's value is reduced and an expense recognized over the accounting periods benefited by the asset's use. See Note 7, Property and Equipment, for additional information on property and equipment held by the House.

The House has possession of numerous assets that may be of significant historical and artistic value. The House does not include these assets in the financial statements. The land and buildings occupied and used by Members, officers, and employees in Washington, D.C. are under the custody of the Architect of the Capitol and are not included in the financial statements of the House.

#### **H. Leases**

The House leases office space, vehicles, computers and other equipment. These leases are generally classified as operating leases. House regulations require that leases entered into by Members for space and vehicles be no longer than the elected term of the Member. The House also enters into leases, which are structured such that their terms effectively finance the purchase of the item. Such leases convey the benefits and risks of ownership and are classified as capital leases, if the net present value of the minimum lease payments due at lease inception meets House capitalization criteria. Items acquired by capital leases are recorded as House assets. The asset and corresponding liability are recorded at the net present value of the minimum lease payments at lease inception. The portion of capital lease payments representing imputed interest is expensed as interest on capital leases. See Note 8, Lease Commitments, for additional lease information.

#### **I. Deferred Credits**

The House receives advance payments from other Federal government entities for shared services, in advance of the delivery of these services. These advance payments are recorded as deferred credits. As the services are rendered the deferred credit account is drawn down and the appropriate revenue is recognized.

#### **J. Revenue from Operations**

Revenue is recognized when goods have been delivered or services rendered.

- Sales of goods consist of Gift Shop and Supply Store sales.
- Sales of services to the public are comprised of Photography sales, Child Care fees, and Attending Physician fees.
- Interoffice sales between House entities consist of computer services, telecommunications, office supplies, framing, recording, office equipment, photography, tape duplication charges, and are eliminated on the consolidating financial statements.
- Other revenue consists of Page School room and board, and vendor commissions.

#### **K. Appropriations to Cover Expenses**

Like other Federal government organizations, the House finances most of its operations with appropriations. The expenses of Members, Committees, and Leadership offices are entirely financed with appropriations. Other House entities require appropriations to the extent the revenue generated does not cover expenses. Appropriations are considered a financing source, not a revenue, since appropriations do not result from an earnings process.

#### **L. Postage and Delivery**

Postage and delivery consists of franked mail expenses and miscellaneous postage expenses. Members' postage includes the use of the Frank, which is charged to the Members' Representational Allowance. Miscellaneous postage expenses include courier charges, stamps, and rental of post office boxes.

#### **M. Repairs and Maintenance**

Repairs and maintenance include all expenses related to the maintenance and upkeep of House equipment in both Washington, D.C. and in Members' district offices, as well as related operating lease payments on various types of equipment. In addition, property and equipment purchases below the capitalization thresholds discussed in Note 2G, Property and Equipment, are classified as repairs and maintenance.

#### **N. Depreciation and Amortization**

The cost of capital assets is allocated ratably over an asset's useful life as depreciation or amortization expense. The

House calculates depreciation and amortization expense based on the straight-line method over an asset's estimated useful life. Depreciation expense is applicable to tangible assets such as furniture, equipment, and vehicles. Amortization expense is applicable to intangible assets such as software and capital leases. Assets acquired under capital leases are generally amortized over the lease term. However, if a lease agreement contains a bargain purchase option or otherwise transfers title of the asset to the House, the asset is amortized on the same basis as similar categories of owned assets.

#### **O. Rent, Utilities, and Communications**

Rent and utilities consist primarily of the rental of district offices by Members and any related utility payments. Communications costs consist of charges for news wire services, satellite fees, and external network access services.

#### **P. Telecommunications**

Telecommunications expense includes local and long distance telephone service in Washington, D.C. and in Members' district offices.

#### **Q. Supplies and Materials**

Supplies and materials include office supplies used by the House and medical supplies used by the Attending Physician. Supplies and materials do not include inventories held for sale by retail entities such as the *Gift Shop* and the *Supply Store*.

#### **R. Travel and Transportation**

Travel and transportation expenses include official travel by Members, Committees, and Leadership offices; travel by other House officers and employees and congressional delegations; freight and shipping costs; and expenses related to the lease and maintenance of vehicles.

#### **S. Contract, Consulting, and Other Services**

Contract, consulting, and other services include the cost of management services in House Postal Operations, annual audit fees, the cost of studies and analyses requested by Committees, as well as computer, recording, janitorial, and catering services.

#### **T. Printing and Reproduction**

This category primarily includes printing and reproduction of constituent communications. Also included are photography services, and printing and reproduction of

items such as informational publications and reference materials.

#### **U. Subscriptions and Publications**

Subscriptions and publications include the cost of periodicals and news services.

#### **V. Cost of Goods Sold**

Cost of goods sold includes the cost of products sold in the retail operations of the *Gift Shop* and the *Supply Store*, and the cost of services provided to federal and non-federal entities, such as the House postal facility.

#### **W. Loss or Gain on Disposal of Assets**

A loss is recognized when the net book value of the asset at the time of disposal exceeds any proceeds received. A gain is recognized when the net book value of the asset at the time of disposal is less than any proceeds received.

#### **X. Annual Leave**

Annual leave for the House Officers and their employees is accrued as earned, and the liability is reduced as leave is taken. The accrued annual leave balance as of September 30, 2006 is calculated according to Public Law 104-53, November 19, 1995, 109 Stat. 514. See Note 10, Accrued Payroll and Benefits and Leave, for additional information.

#### **Y. Federal Employee and Veterans Benefits**

This benefit expense includes the current cost of providing future pension benefits to eligible employees at the time the employees' services are rendered. Also included is the current period expense for the future cost of providing retirement benefits and life insurance to House employees. See Note 16, Benefits, for additional information.

#### **Z. Use of Estimates**

The preparation of financial statements requires management to make estimates and assumptions that affect the reported amount of assets and liabilities, as well as the disclosure of contingent assets and liabilities at the date of the financial statements, and the amount of revenue and expense reported during the period. Actual results could differ from those estimates.

### NOTE 3 - INTRA-GOVERNMENTAL FINANCIAL ACTIVITIES

The House has significant intra-governmental financial activities with Executive and Legislative Branch entities. These financial activities include transactions and agreements to purchase goods and services.

#### Transactions with Executive Branch Agencies

The House's most significant interagency transactions are with the:

- U.S. Postal Service for postage.
- Department of Defense for contractual and maintenance services
- U.S. Department of Labor (DOL) for unemployment and workers' compensation.
- General Services Administration (GSA) for the use and upkeep of office space in certain Members' district offices, office supplies and leased vehicles.
- U.S. Department of the Interior, U.S. Geological Survey, National Business Center for financial system contract and consulting services.
- U.S. Department of Transportation for transit benefits program.
- Other Executive Branch agencies for special studies as requested by House Committees.

Significant cash disbursements to Executive Branch agencies during the fiscal years ended September 30, 2006 and 2005 were approximately:

Disbursements to Executive Branch Agencies	2006	2005
U.S. Postal Service	\$ 32,466,000	\$ 16,383,000
Department of Defense	513,000	2,840,000
General Services Administration	4,399,000	4,442,000
U.S. Department of Labor	2,157,000	2,645,000
U.S. Department of Transportation	1,856,000	1,535,000
U.S. Department of the Interior	519,000	517,000
Other Executive Branch Agencies	93,000	259,000

The House also reports significant financial transactions with the U.S. Department of State, which maintains and

administers the Congressional Use of Foreign Currency account on behalf of Congress. This account, which was established in 1948 and made permanent in 1981, is authorized by legislation codified in Title 22, Sec. 1754 of the United States Code. The funds are available to Congressional Committees and delegations to cover local currency expenses incurred while traveling abroad. The fund balance related to the account is included in Fund Balance with U.S. Treasury under Officers and Legislative Offices.

Use of the foreign currency account for Congressional delegations and other official foreign travel of the House is authorized by either the Speaker of the House or the chairman of a Standing, Special and Select, or Joint Committee. Therefore, all foreign currency account financial activity is reported as Committee and Leadership office travel expense.

Foreign Currency Balance with the U.S. Department of State	2006	2005
Beginning Balance	\$ 21,132,955	\$ 11,688,215
Appropriation Received	15,000,000	18,000,000
Travel Expenses:		
Leadership	(1,505,669)	(1,504,870)
Committees	(7,708,954)	(7,050,390)
Ending Balance	<u>\$ 26,918,332</u>	<u>\$ 21,132,955</u>

#### Transactions with Legislative Branch Entities

The House pays for support services provided by other Legislative Branch entities. These entities receive their own appropriations and operate autonomously from the House's administrative functions. The House received support services from the United States Senate in 2006. The House also receives support services from the Government Printing Office and the Architect of the Capitol.

Cash Disbursements to Legislative Branch Entities	2006	2005
Architect of the Capitol	\$ 233,000	\$ 243,000
Government Printing Office	79,000	150,000
United States Senate	967,000	546,000

The House also receives payments for services provided to the Congressional Budget Office and the Architect of the

Capitol and for the reimbursement of services shared with other Federal government entities. In 2006 and 2005, the House shared services with the Library of Congress, and the United States Senate.

<b>Cash Receipts from Legislative Branch Entities</b>	<b>2006</b>	<b>2005</b>
Library of Congress	\$ 4,120,000	\$ 3,872,000
United States Senate	315,000	403,000
Architect of the Capitol	294,000	327,000
Congressional Budget Office	93,000	91,000

## NOTE 4 - FUND BALANCE WITH THE U.S. TREASURY AND CASH

The House has appropriated and revolving fund balances with the U.S. Treasury. The balances, as of September 30, 2006 and 2005 were:

<b>Fund/Cash Accounts Maintained by the House</b>	<b>2006</b>	<b>2005</b>
Fund Balance with Treasury/Cash	\$ 147,788,790	\$ 190,880,997
Congressional Use of Foreign Currency	<u>26,918,332</u>	<u>21,132,955</u>
Total	<u>\$ 174,707,122</u>	<u>\$ 212,013,952</u>

The House usually receives the full amount of its appropriation at the beginning of each fiscal year.

Cash on Hand represents deposits in transit and amounts held in a commercial bank account. Cash on Hand was \$1,673 and \$120 as of September 30, 2006 and 2005, respectively.

## NOTE 5 - ACCOUNTS RECEIVABLE

Accounts Receivable balances represent amounts owed the House by Federal agencies, Members, employees and/or vendors less an allowance for doubtful accounts. The Allowance for Doubtful Accounts was derived from the receivables amount owed to the House for more than six months. The House is actively pursuing these overpayments.

<b>Accounts Receivable</b>	<b>2006</b>	<b>2005</b>
Accounts Receivable	\$ 1,367,102	\$1,307,729
Less: Allowance for Doubtful Accounts	<u>(621,303)</u>	<u>(166,021)</u>
Accounts Receivable, Net	<u>\$ 745,799</u>	<u>\$1,141,708</u>

## NOTE 6 - ADVANCES AND PREPAYMENTS

Advances and prepayments are transfers of cash to cover future expenses or the acquisition of assets. These goods and/or services are delivered in increments that span several months. Advance payments are recorded as assets. As the goods and/or services are rendered, the Advance account is drawn down and the appropriate asset or expense is recognized. Prepayments are made for subscriptions and software licenses and are charged as expenses. At year-end, all such payments made for the previous, current and

succeeding years are analyzed to determine the proper expense and prepayment amounts applicable to the current accounting period for financial statement purposes. Advances and Prepayments are:

	<b>2006</b>	<b>2005</b>
Advances	\$ 90,878	\$ 100,010
Prepayments	<u>2,616,481</u>	<u>3,955,961</u>
Total	<u>\$ 2,707,359</u>	<u>\$ 4,055,971</u>

**NOTE 7 – PROPERTY AND EQUIPMENT**

Software, and vehicles and equipment, including computers, are capitalized if their acquisition cost equals or exceeds \$10,000 and \$25,000, respectively. Work in process consists of capitalized costs associated with assets received, but not placed in service as of the fiscal year end. Depreciation and

amortization expense is based on the straight-line method over an asset's estimated useful life. The change in work in process is due to numerous assets placed in service during the fiscal year. Property and equipment as of September 30, 2006 and the related depreciation and amortization expense are:

<b>2006 Classes of Property and Equipment</b>	<b>Service Life (Years)</b>	<b>Estimated Acquisition Value</b>	<b>Accumulated Amortization/ Depreciation</b>	<b>Estimated Net Book Value</b>	<b>Amortization/ Depreciation Expense</b>
Work in Process	N/A	\$ 2,985,986	\$ -	\$ 2,985,986	\$ -
Computer Software and Hardware	3	88,136,004	69,523,012	18,612,992	12,731,001
Computer Software and Hardware	5	790,911	790,911	-	-
Equipment	5	39,214,760	26,442,339	12,772,421	5,074,480
Motor Vehicles	5	10,474,287	3,087,032	7,387,255	2,094,857
Furnishings and Other Equipment	10	1,816,568	1,626,757	189,811	58,320
Assets Under Capital Lease	10	1,354,473	372,479	981,994	135,447
Leasehold Improvements	10	8,971,191	3,057,445	5,913,746	830,185
<b>Total</b>		<b>\$ 153,744,180</b>	<b>\$ 104,899,975</b>	<b>\$ 48,844,205</b>	<b>\$ 20,924,290</b>

Property and equipment as of September 30, 2005 and the related depreciation and amortization expense are:

<b>2005 Classes of Property and Equipment</b>	<b>Service Life (Years)</b>	<b>Estimated Acquisition Value</b>	<b>Accumulated Amortization/ Depreciation</b>	<b>Estimated Net Book Value</b>	<b>Amortization/ Depreciation Expense</b>
Work in Process	N/A	\$ 4,827,236	\$ -	\$ 4,827,235	\$ -
Computer Software and Hardware	3	83,776,443	62,497,452	21,278,991	15,663,146
Computer Software and Hardware	5	790,911	790,911	-	-
Equipment	5	35,426,553	22,780,542	12,646,011	4,492,100
Motor Vehicles	5	10,278,798	998,495	9,280,303	575,398
Furnishings and Other Equipment	10	1,710,068	1,568,300	141,768	61,778
Assets Under Capital Lease	10	1,354,473	237,033	1,117,440	135,447
Leasehold Improvements	10	7,503,829	2,211,342	5,292,487	709,260
<b>Total</b>		<b>\$ 145,668,311</b>	<b>\$ 91,084,075</b>	<b>\$ 54,584,235</b>	<b>\$ 21,637,129</b>



**NOTE 8 – LEASE COMMITMENTS****Capital Leases**

The House enters into leases, which are structured such that their terms effectively finance the purchase of the item. Such leases convey the benefits and risks of ownership and are classified as capital leases, if the net present value of the future minimum lease payments due at lease inception meets House capitalization criteria. Items acquired by capital leases are recorded as House assets. The asset and corresponding liability are recorded at the net present value of the future minimum lease payments due at lease inception. Assets under capital leases consist solely of building structures. An adjustment was made to decrease capital lease liability to reflect the correct value of the asset under capital lease.

Future Capital Lease Payments Due as of September 30, 2006:

Year	
2007	\$ 301,428
2008	301,428
2009	301,428
2010	301,428
2011	301,428
Thereafter	678,213
Total Future Capital Lease Payments	\$2,185,353
Less: Imputed Interest	(997,101)
Net Capital Lease Liabilities	\$1,188,252
Unfunded Liability	\$1,188,252

**Operating Leases**

The House enters into various operating leases for temporary usage of office space, vehicles, hardware, and software. Leases that convey the benefits and risks of

ownership, but do not meet House capitalization criteria are also recognized as operating leases. Operating lease payments are recorded as expenses. Future operating lease payments are not accrued as liabilities. Members may lease office space in their districts through GSA or may directly lease space from the private sector. The Members' Congressional Handbook states that a Member cannot enter into a lease for office space beyond his/her elected term. Members and officers also enter into leases to rent vehicles for official business purposes. A Member may lease a vehicle for a period that exceeds the current congressional term, but the Member remains personally responsible for the lease liability if service to the House concludes prior to lease termination. House administration also leases hardware and software.

Future Operating Lease Payments Due as of September 30, 2006:

Year	Vehicles	Office Space	Parking	Total
2007	\$ 498,739	\$ 5,752,528	\$ 6,267	\$ 6,251,267
2008	110,471	18,458	1,580	128,929
	\$ 609,210	\$ 5,770,986	\$ 7,847	\$ 6,380,196

Lease expense for office space was \$22,640,564 and \$23,225,275 for the years ended September 30, 2006 and 2005, respectively. Lease expense for vehicles was \$1,661,266 and \$1,791,027 for the years ended September 30, 2006 and 2005, respectively.

**NOTE 9 - ACCOUNTS PAYABLE**

Accounts Payable balances represent amounts owed for the cost of goods and services received but not yet paid. Accounts Payable also includes amounts owed to DOL for unemployment compensation.

Accounts Payable	2006	2005
Vendor Payables	\$ 31,526,737	\$ 25,102,588
Unemployment Compensation	159,876	253,782
Total	\$ 31,686,613	\$ 25,356,370

## NOTE 10 - ACCRUED PAYROLL AND BENEFITS AND LEAVE

The House has both funded and unfunded payroll, benefits and leave. A funded liability has a corresponding appropriation to liquidate it. An unfunded liability is a liability that is incurred during the current or prior year but is not payable until a future fiscal year for which an appropriation has not yet been received.

The accrued annual leave balances are calculated according to Public Law 104-53, November 19, 1995, Sec. 109 Stat. 522 (i.e., the lesser of the employee's monthly pay or the monthly pay divided by 30 days and multiplied by the number of days of accrued leave). Sick and other types of paid leave are expensed as they are taken. Accrued payroll and benefits include salaries and associated benefits earned in September and paid in October.

The Members' and Committees' Congressional Handbooks allow offices to adopt personnel policies that provide for the accrual of annual leave and use of such leave. Leadership offices have also adopted similar policies. While leave is tracked from one pay period to the next, a consistent policy has not been formally adopted by these entities regarding

the accrual and payment of leave time. Therefore, an accrued leave liability for Members, Committees, and Leadership offices is estimated on the financial statements. Accrued Workers' Compensation is the amount billed by Department of Labor that will be paid in subsequent fiscal years.

Accrued annual leave and accrued payroll and benefits as of September 30, 2006 and 2005 were:

<b>Accrued Leave, Payroll and Benefits, and Workers' Compensation</b>	<b>2006</b>	<b>2005</b>
<b>Funded</b>		
Accrued Payroll and Benefits	\$ 8,057,874	\$ 7,755,802
<b>Unfunded</b>		
Accrued Annual Leave	8,225,229	7,543,151
Accrued Workers' Compensation	2,316,913	1,862,312
<b>Total Unfunded</b>	<b>\$ 10,542,142</b>	<b>\$ 9,405,463</b>

## NOTE 11 - DEFERRED CREDITS

The House received payments in advance of receipt of shared services from the Library of Congress, the Senate and the Department of State. The deferred credit balance as of

September 30, 2006 and 2005 was \$720,599 and \$903,087, respectively.

## NOTE 12 - UNFUNDED WORKERS' COMPENSATION ACTUARIAL LIABILITY

The Federal Employees' Compensation Act (FECA) provides income and medical cost protection to covered Federal civilian employees injured on the job, employees who have incurred a work-related occupational disease, and beneficiaries of employees whose death is attributable to a job-related injury or occupational disease. Claims incurred for the benefit of House employees under FECA are administered by DOL, which pays the initial claim and obtains reimbursement from the House. The unfunded workers' compensation actuarial liability is an estimate based on actuarial calculations using

historical payment patterns to predict what costs will be incurred in the future. The liability is adjusted annually by applying actuarial procedures. Any upward or downward adjustment to the liability is recorded as an annual increase or decrease to benefits expense. The House calculated the actuarial liability based on a model developed by DOL. The projected Unfunded Workers' Compensation Actuarial Liabilities as of September 30, 2006 and 2005 were \$19,610,394 and \$18,537,652, respectively.

**NOTE 13 - NET POSITION**

The components of Net Position are:

- Unexpended Appropriations - Appropriations are not considered expended until goods have been received or services have been rendered.
- Total Cumulative Results of Operations:

Cumulative Results of Operations - The net difference between expenses and revenue and financing sources including appropriations, revenues from operations and imputed financing sources.

Invested Capital - Funds used to finance capital assets such as computer hardware and software, vehicles, equipment, and inventory.

Future Funding Requirements - Known liabilities to be funded by future appropriations for accrued Annual Leave and Workers' Compensation.

Unexpended appropriations cancel at the end of the second fiscal year following the year in which appropriated. As required by law, these funds must be returned to the U.S. Treasury general account. Funds that were canceled and returned to the U.S. Treasury during fiscal years 2006 and 2005 are:

Appropriations	2006	2005
2004	\$ 7,689,345	
2003	-	7,753,623
Total	\$ 7,689,345	\$ 7,753,623

**Net Position** as of September 30, 2006 and 2005 for Appropriated Funds and Revolving Funds, including the House Recording Studio, Net Expenses of Equipment, Page School, House Services, Net Expenses of Telecommunications, and Office Supply Service revolving funds are shown in the following table:

Net Position	Net Position September 30, 2006 Totals		Net Position September 30, 2005 Totals	
Unexpended Appropriations		\$ 121,516,521		\$ 166,493,777
Cumulative Results of Operations:				
Cumulative Results of Operations	\$ 15,208,811		\$ 16,316,138	
Invested Capital	50,112,194		54,662,719	
Future Funding Requirements	(30,170,036)		(27,943,114)	
Total Cumulative Results of Operations		35,150,969		43,035,743
Total Net Position		\$ 156,667,490		\$ 209,529,520

Changes in net position may include prior period adjustments, excesses or shortages of revenue and financing sources over expenses, and non-operating changes, such as investments in capital assets and inventory. Increases (or decreases) in non-operating changes result when amounts invested in capital assets and inventory exceed (or are less

than) the amounts of liabilities to be funded by future appropriations.

The Net Position table above reflects an additional cumulative results of operations line which further disaggregates activity other than invested capital or future funding requirements.

## NOTE 14 - REVOLVING FUNDS, INTEROFFICE SALES, AND TRANSFERS

Some House entities transfer costs to Members, Committees, and other House offices for goods and services provided. These entities are primarily:

- House Support Services, which transfers costs of equipment to the Members and Committees,
- House Information Resources, which transfers telecommunication charges, and
- Office Supply Service, which transfers office supply purchases and flag sales.

Some House business-like entities operate as revolving funds. A revolving fund is a budgetary structure established by statute that authorizes certain government agencies to collect user fees or revenue to finance operating expenses. In 2006, the House operated revolving fund type activities for the House Recording Studio, Net Expenses of Equipment, Page School, Office Supply Service, Child Care Center, House Services, and Net Expenses of Telecommunications..

## NOTE 15 - APPROPRIATIONS TO COVER EXPENSES

**Appropriations Received** include current and prior year funds necessary to finance House operating expenses such as personnel and benefits costs, contract services, and travel expenses. The House recognizes appropriations to cover expenses in the same period in which the associated expense is incurred. Appropriations to cover investments in capital assets and inventory are recognized in the same period in which they are received.

**Appropriations Yet To Be Received** consist of expenses that are incurred in the current period, but will be funded by future appropriations. Such amounts include accrued actuarial liabilities, annual leave and workers' compensation expenses.

## NOTE 16 - BENEFITS

House Members and employees are covered by either the Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS). Both Members and employees are eligible for retirement benefits under CSRS or FERS. A CSRS basic annuity, unreduced for age, debts to the fund, or survivor's benefits, is calculated by multiplying the highest 3 consecutive years' average salary by a percentage factor which is based on the length of Federal service. However, Members' benefits are different from those of employees. For example, a Member covered by CSRS is eligible to receive unreduced retirement benefits at age 60 if he or she has 10 years of Member service. An employee is eligible to receive reduced benefits at age 50 with 20 years of service or at any age with 25 years of service. The FERS basic benefit plan provides the same benefits for either Members or employees.

CSRS employees contribute a portion of their earnings to the Civil Service Retirement Fund. The House also contributes an amount to this fund. FERS employees, in addition to paying Social Security, contribute a portion of their base earnings to the FERS retirement fund. The House also contributes an amount toward the FERS retirement and Social Security funds.

Both FERS and CSRS employees can contribute to the Thrift Savings Plan (TSP) up to the IRS limit. FERS employees also receive an automatic one percent House-paid contribution, as well as an additional House matching TSP contribution up to five percent of their basic pay. CSRS employee contributions to TSP do not receive matching House contributions. FERS employees could receive benefits from FERS, the Social Security System, and TSP. CSRS employees could receive benefits from CSRS and TSP.

Member and Employee Expenses	2006	2005
Retirement Plan Contributions	\$ 130,955,863	\$ 125,198,418
Federal Employee and Veterans' Benefits	57,557,337	53,898,845
Social Security	45,906,604	43,012,110
Health Insurance	42,311,529	39,616,471
Student Loan/Fitness Center Programs	8,821,612	7,790,571
Unemployment and Workers' Compensation	1,580,366	2,024,032
Annual Leave	682,079	970,105
Death Benefits	1,303,657	899,705
Transit Benefits	2,030,798	1,744,572
Life Insurance	1,074,826	1,009,194
Workers' Compensation Actuarial Adjustment	1,385,042	1,573,327
Total	<u>\$ 293,609,713</u>	<u>\$ 277,737,350</u>

Benefits costs for the past 3 years have averaged approximately \$279 million per year.

Federal-employing entities recognize their share of the cost of providing future pension benefits to eligible employees at the time the employees' services are rendered. This cost is included in Federal Employee and Veterans' Benefits expense. The pension expense recognized in the Statement of Operations is the current service cost for House employees less the amount contributed by the employee.

The measurement of the service cost requires the use of actuarial cost methods and assumptions, with the factors applied by the House provided by the Office of Personnel Management (OPM), the federal agency that administers the plan. The excess of the recognized pension expense over the amount contributed by the House represents the amount being financed directly through the Civil Service Retirement and Disability Fund administered by OPM.

## NOTE 17 - EMERGENCY PREPAREDNESS

The House continues to develop contingency plans to ensure the continuation of all House Operations in the event of an emergency evacuation.

## NOTE 18 - CONTINGENCIES

The House is currently involved in two lawsuits, the probable outcomes of which are unfavorable. The amount of the first lawsuit has been estimated as an immaterial amount which has been included in Other Liabilities. The

The House does not receive an appropriation to fund this expense. Therefore, this portion of the pension expense is considered an imputed financing source to the House, and is included in the Imputed Financing Sources on the Statement of Operations. This amount was \$12,163,174 in 2006 and \$12,559,394 in 2005.

Federal-employing entities also recognize a current period expense for the future cost of post-retirement health benefits and life insurance for its employees while they are still employed. This cost is included in Federal Employee and Veterans' Benefits expense in the Statement of Operations. Employees and the House do not currently make contributions to fund these future benefits, and the House does not receive an appropriation to fund this expense. Therefore, this portion of the post-retirement health benefits and life insurance is considered an imputed financing source to the House, and is included in Imputed Financing Sources on the Statement of Operations. This amount was \$45,394,163 in 2006 and \$41,339,451 in 2005.

Federal Employee and Veterans' Benefits (Imputed Financing Source)	2006	2005
Current Service Cost - Federal Employees Health Benefits	\$45,288,369	\$41,239,133
Current Service Cost - Federal Pensions	12,163,174	12,559,394
Current Service Cost - Federal Employees Group Life Insurance	105,794	100,318
Total	<u>\$57,557,337</u>	<u>\$53,898,845</u>

Approximately \$30 million and \$33 million were expended in 2006 and 2005, respectively.

precise amount for the second lawsuit is unknown based on the best information available as of the reporting date and is not reflected in the financial statements.

This Page Intentionally Left Blank

## **Supplemental Financial Schedules**

This Page Intentionally Left Blank



# **Organization and Composition of Financial Statements**

This Page Intentionally Left Blank

**U.S. House of Representatives  
Organization and Composition of  
Consolidating Financial Statements**

**Members**

Representatives, Delegates and Resident  
Commissioner  
Members' Allowances and Expenses

Legislative Computer Systems  
Office of Legislative Operations  
Legislative Resource Center  
Official Reporters  
Office of Publication Services  
Capitol Service Groups

**Committees**

Committee on Agriculture  
Committee on Appropriations  
Committee on Armed Services  
Committee on the Budget  
Committee on Education and the Workforce  
Committee on Energy and Commerce  
Committee on Financial Services  
Committee on Government Reform  
Committee on Homeland Security  
Committee on House Administration  
Committee on International Relations  
Committee to Investigate the Preparation for and  
Response to Hurricane Katrina  
Committee on the Judiciary  
Committee on Resources  
Committee on Rules  
Committee on Science  
Committee on Small Business  
Committee on Standards of Official Conduct  
Committee on Transportation and Infrastructure  
Committee on Veterans' Affairs  
Committee on Ways and Means  
Permanent Select Committee on Intelligence

Office of the Sergeant at Arms  
Immediate Office  
Chamber Security  
Capitol Guide Service and Congressional Special  
Services Office  
House Garages and Parking Security

Chief Administrative Officer (CAO)  
Immediate Office  
Press Gallery  
Periodical Press Gallery  
Radio/TV Correspondents' Gallery  
CAO Business Improvement Team

House Information Resources  
Client Services Group  
Communications Group  
Information Management

Office of Human Resources  
Office of Employee Assistance  
ADA Services  
Child Care  
Office of Administration  
Outplacement Services  
Office of Training

**Leadership Offices**

Office of the Speaker  
Office of the Majority Leader  
House Majority Whip  
Office of the Democratic Leader  
Democratic Whip  
House Republican Conference  
House Republican Policy Committee  
Democratic Caucus

House Support Services (HSS)  
Contractor Management  
Furniture Support Services  
House Office Service Center  
First Call Customer Service Center  
House Gift Shop  
Mail List/Processing/ Mass Mail  
Office Supply Service  
Office Services  
Special Events  
House Recording Studio  
Operations Support Center  
Acquisition and Account Management

**Officers and Legislative Offices**

Office of the Clerk  
Immediate Office  
Office of History and Preservation  
Office of House Employment Counsel  
House Page Program

Central Receiving/Warehouse	House Recording Studio
Logistics and Distribution	Page School Revolving Fund
Vendor Management	
Production Management	Office of the Chaplain
Photography	Office of Interparliamentary Affairs
	Parliamentarian
Office of Finance and Procurement	Office of the Parliamentarian
Accounting	Compilation of Precedents
Budget	Office of the Law Revision Counsel
Financial Counseling	Office of the Legislative Counsel
Office of Personnel and Benefits	Office of the General Counsel
Payroll	Office of Inspector General
Office of Member Services	Office of Emergency Planning, Preparedness and
Financial Systems	Operations
Procurement	Office of House Historian
	Technical Assistants to the Attending Physician
Revolving Funds	Congressional Executive Commission on the
Child Care Center	People's Republic of China
House Services	Commission on Security and Cooperation in Europe
House Beauty Shop	
House Barber Shop	
House Restaurant	
Stationery	
	<b>Joint Functions</b>
	Office of the Attending Physician
	Joint Committee on Taxation

## **Consolidating Statements**

**U.S. House of Representatives**  
**Consolidating Statement of Financial Position**  
**as of September 30, 2006**

	<u>Members</u>	<u>Committees</u>
<b>ASSETS</b>		
Fund Balance with U.S. Treasury	\$ 18,900,392	\$ 6,724,615
Cash	<u>0</u>	<u>0</u>
Fund Balance with U.S. Treasury and Cash	18,900,392	6,724,615
Accounts Receivable, Net	289,098	9,120
Interoffice Receivable	0	0
Advances and Prepayments	1,016,659	255,947
Inventory	0	0
Property and Equipment, Net	<u>272,534</u>	<u>3,575,062</u>
Total Assets	<u>\$ 20,478,683</u>	<u>\$ 10,564,744</u>
<b>LIABILITIES AND NET POSITION</b>		
Accounts Payable	\$ 10,020,849	\$ 1,637,593
Interoffice Payable	1,340,845	223,567
Capital Lease Liabilities	0	0
Accrued Funded Payroll and Benefits	7,568,874	1,093
Accrued Unfunded Annual Leave and Workers' Compensation	4,746,056	1,596,800
Deferred Credits	0	0
Unfunded Workers' Compensation Actuarial Liability	0	0
Other Liabilities	<u>0</u>	<u>0</u>
Total Liabilities	<u>23,676,624</u>	<u>3,459,053</u>
Unexpended Appropriations	1,302,984	5,160,477
Cumulative Results of Operations	<u>(4,500,925)</u>	<u>1,945,214</u>
Total Net Position	<u>(3,197,941)</u>	<u>7,105,691</u>
Total Liabilities and Net Position	<u>\$ 20,478,683</u>	<u>\$ 10,564,744</u>

<b>Leadership Offices</b>	<b>Officers and Legislative Offices</b>	<b>Joint Functions</b>	<b>Eliminations</b>	<b>Combined</b>
\$ 3,373,923	\$ 143,625,927	\$ 2,080,592	\$ 0	\$ 174,705,449
0	1,673	0	0	1,673
<u>3,373,923</u>	<u>143,627,600</u>	<u>2,080,592</u>	<u>0</u>	<u>174,707,122</u>
15,314	432,141	126	0	745,799
0	1,735,206	0	(1,735,206)	0
56,793	1,307,342	70,618	0	2,707,359
0	1,883,757	0	0	1,883,757
<u>209,320</u>	<u>44,009,641</u>	<u>777,648</u>	<u>0</u>	<u>48,844,205</u>
<u>\$ 3,655,350</u>	<u>\$ 192,995,687</u>	<u>\$ 2,928,984</u>	<u>\$ (1,735,206)</u>	<u>\$ 228,888,242</u>
\$ 420,756	\$ 18,814,615	\$ 792,800	\$ 0	\$ 31,686,613
56,273	107,261	7,260	(1,735,206)	0
0	1,188,252	0	0	1,188,252
0	487,544	363	0	8,057,874
158,844	4,017,586	22,856	0	10,542,142
0	720,599	0	0	720,599
0	19,610,394	0	0	19,610,394
<u>0</u>	<u>414,878</u>	<u>0</u>	<u>0</u>	<u>414,878</u>
<u>635,873</u>	<u>45,361,129</u>	<u>823,279</u>	<u>(1,735,206)</u>	<u>72,220,752</u>
2,969,001	111,300,205	783,854	0	121,516,521
<u>50,476</u>	<u>36,334,353</u>	<u>1,321,851</u>	<u>0</u>	<u>35,150,969</u>
<u>3,019,477</u>	<u>147,634,558</u>	<u>2,105,705</u>	<u>0</u>	<u>156,667,490</u>
<u>\$ 3,655,350</u>	<u>\$ 192,995,687</u>	<u>\$ 2,928,984</u>	<u>\$ (1,735,206)</u>	<u>\$ 228,888,242</u>

**U.S. House of Representatives**  
**Consolidating Statement of Operations**  
**for the Year Ended September 30, 2006**

	<u>Members</u>	<u>Committees</u>
<b>REVENUE AND FINANCING SOURCES</b>		
Revenue from Operations		
Sales of Goods	\$ 0	\$ 0
Sales of Services to Federal Entities	0	0
Sales of Services to the Public	0	0
Interoffice Sales	0	0
Other Revenue	0	0
Total Revenue from Operations	0	0
Financing Sources		
Appropriations to Cover Expenses:		
Appropriations Received	794,455,757	198,087,987
Appropriations Yet To Be Received	1,478,236	533,405
Imputed Financing Source	37,153,685	11,145,245
Total Revenue and Financing Sources	\$ 833,087,678	\$ 209,766,637
<b>EXPENSES</b>		
Personnel Compensation	\$ 463,948,085	\$ 127,785,206
Benefits	192,663,828	54,323,919
Postage and Delivery	33,563,246	35,125
Repairs and Maintenance	23,167,909	4,406,320
Depreciation and Amortization	280,356	1,622,413
Rent, Utilities, and Communications	24,911,329	75,718
Telecommunications	15,372,716	2,002,151
Supplies and Materials	9,187,352	1,285,804
Travel and Transportation	23,462,155	9,642,368
Contract, Consulting, and Other Services	8,621,745	6,632,705
Printing and Reproduction	28,160,402	148,336
Subscriptions and Publications	9,446,102	1,482,580
Cost of Goods Sold	0	0
Other Expenses	22,942	291,329
Bad Debts	279,511	32,663
Interest on Capital Leases	0	0
Total Expenses	\$ 833,087,678	\$ 209,766,637
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	\$ 0	\$ 0
<b>CHANGE IN NET POSITION</b>		
Net Position, Beginning Balance	\$ 5,688,523	\$ 7,200,134
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	0	0
Plus (Minus) Non-Operating Changes	(8,886,464)	(94,443)
Net Position, Ending Balance	\$ (3,197,941)	\$ 7,105,691



<b>Leadership Offices</b>	<b>Officers and Legislative Offices</b>	<b>Joint Functions</b>	<b>Eliminations</b>	<b>Combined</b>
\$ 0	\$ 2,817,117	\$ 0	\$ 0	\$ 2,817,117
0	4,772,769	0	0	4,772,769
0	906,061	119,852	0	1,025,913
0	33,513,505	0	(33,513,505)	0
0	662,440	0	0	662,440
0	42,671,892	119,852	(33,513,505)	9,278,239
27,346,608	217,834,756	13,703,131	0	1,251,428,239
22,862	2,017,010	4,406	0	4,055,919
1,435,028	7,222,689	600,690	0	57,557,337
\$ 28,804,498	\$ 269,746,347	\$ 14,428,079	\$ (33,513,505)	\$ 1,322,319,734
\$ 16,433,826	\$ 82,769,626	\$ 6,887,933	\$ 0	\$ 697,824,676
6,953,187	36,644,982	3,023,797	0	293,609,713
13,517	349,251	3,367	0	33,964,506
866,088	24,377,525	528,873	0	53,346,715
169,261	18,276,550	575,710	0	20,924,290
48,807	1,429,224	409	0	26,465,487
853,496	8,963,293	110,661	0	27,302,317
729,852	3,751,930	413,070	0	15,368,008
1,774,582	1,564,146	47,658	0	36,490,909
370,663	49,223,432	2,520,972	0	67,369,517
144,230	53,161	2,077	0	28,508,206
377,527	619,157	192,800	0	12,118,166
0	39,748,679	0	(33,513,505)	6,235,174
55,557	142,165	0	0	511,993
13,905	40,831	900	0	367,810
0	230,927	0	0	230,927
\$ 28,804,498	268,184,879	\$ 14,308,227	\$ (33,513,505)	\$ 1,320,638,414
\$ 0	\$ 1,561,468	\$ 119,852	\$ 0	\$ 1,681,320
\$ 2,341,627	\$ 192,044,944	\$ 2,254,292	\$ 0	\$ 209,529,520
0	1,561,468	119,852	0	1,681,320
677,850	(45,971,854)	(268,439)	0	(54,543,350)
\$ 3,019,477	\$ 147,634,558	\$ 2,105,705	\$ 0	\$ 156,667,490

**U.S. House of Representatives**  
**Consolidating Statement of Cash Flows**  
**for the Year Ended September 30, 2006**

	<u>Members</u>	<u>Committees</u>
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>		
Excess/(Deficiency) of Revenue and Financing Sources over Expenses	\$ 0	\$ 0
Adjustments affecting Cash Flow		
Appropriations Affecting Cash	(590,285,666)	(152,716,334)
(Increase)/Decrease in Accounts and Interoffice Receivable	525,067	201,967
(Increase)/Decrease in Advances and Prepayments	1,535,028	298,314
(Increase)/Decrease in Inventory	0	0
Increase/(Decrease) in Accounts and Interoffice Payable	597,815	778,770
Increase/(Decrease) in Other Accrued Liabilities	660,056	216,342
(Gain)/Loss on Disposal of Assets	22,942	291,329
Depreciation and Amortization	<u>280,356</u>	<u>1,622,413</u>
Net Cash Provided/(Used) by Operating Activities	<u>(586,664,402)</u>	<u>(149,307,199)</u>
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>		
Purchase of Property and Equipment	<u>(76,843)</u>	<u>(599,960)</u>
Net Cash Provided/(Used) by Investing Activities	<u>(76,843)</u>	<u>(599,960)</u>
<b>CASH FLOWS FROM FINANCING ACTIVITIES</b>		
Appropriations	562,119,000	147,165,930
Funds Returned to the U.S. Treasury	(1,003,398)	(5,558)
Appropriated Funds Allocated	20,156,232	4,270,617
Principal Payment on Capital Lease Liabilities	<u>0</u>	<u>0</u>
Net Cash Provided/(Used) by Financing Activities	<u>581,271,834</u>	<u>151,430,989</u>
Net Cash Provided/(Used) by Operating, Investing, and Financing Activities	(5,469,411)	1,523,830
Fund Balance with U.S. Treasury and Cash, Beginning	<u>24,369,803</u>	<u>5,200,785</u>
Fund Balance with U.S. Treasury and Cash, Ending	<u>\$ 18,900,392</u>	<u>\$ 6,724,615</u>

<b>Leadership Offices</b>	<b>Officers and Legislative Offices</b>	<b>Joint Functions</b>	<b>Eliminations</b>	<b>Combined</b>
\$ 0	\$ 1,561,468	\$ 119,852	\$ 0	\$ 1,681,320
(35,938,639)	(357,908,745)	(12,233,458)	0	(1,149,082,842)
18,920	(764,477)	10,804	403,628	395,909
51,854	(531,792)	(4,792)	0	1,348,612
0	(558,124)	0	0	(558,124)
(45,151)	4,757,489	644,948	(403,628)	6,330,243
(18,422)	1,526,280	(15,231)	0	2,369,025
55,557	124,665	0	0	494,493
169,261	18,276,550	575,710	0	20,924,290
<u>(35,706,620)</u>	<u>(333,516,686)</u>	<u>(10,902,167)</u>	<u>0</u>	<u>(1,116,097,074)</u>
<u>(73,711)</u>	<u>(13,456,397)</u>	<u>(368,525)</u>	<u>0</u>	<u>(14,575,436)</u>
<u>(73,711)</u>	<u>(13,456,397)</u>	<u>(368,525)</u>	<u>0</u>	<u>(14,575,436)</u>
19,344,000	361,269,000	11,227,590	0	1,101,125,520
(722,092)	(5,891,372)	(66,925)	0	(7,689,345)
17,766,868	(43,012,731)	819,014	0	0
0	(70,495)	0	0	(70,495)
<u>36,388,776</u>	<u>312,294,402</u>	<u>11,979,679</u>	<u>0</u>	<u>1,093,365,680</u>
608,445	(34,678,681)	708,987	0	(37,306,830)
<u>2,765,478</u>	<u>178,306,281</u>	<u>1,371,605</u>	<u>0</u>	<u>212,013,952</u>
<u>\$ 3,373,923</u>	<u>\$ 143,627,600</u>	<u>\$ 2,080,592</u>	<u>\$ 0</u>	<u>\$ 174,707,122</u>

This Page Intentionally Left Blank

# **Independent Auditor's Report on Compliance with Laws and Regulations**

This Page Intentionally Left Blank



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

**INDEPENDENT AUDITOR'S REPORT ON  
COMPLIANCE WITH LAWS AND REGULATIONS**

To the Inspector General  
U.S. House of Representatives

Cotton & Company LLP has audited the financial statements for the U.S. House of Representatives (House) as of September 30, 2006 and 2005 for the fiscal years ended and have issued our reports thereon dated April 30, 2007. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Compliance with laws, rules, and regulations is the responsibility of the Members and administrative management of the House. As part of obtaining reasonable assurance about whether the House's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and House rules and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. Providing an opinion on compliance with those provisions was not, however, an objective of our audit and, accordingly, we do not express such an opinion. Results of our tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.

House compliance with laws, rules, and regulations for the House is significantly different than for Executive Branch departments and agencies. First, many laws that apply to the Executive Branch, such as the Federal Managers' Financial Integrity Act of 1982, Government Management Reform Act of 1994, and Chief Financial Officers Act of 1990, do not apply to the House. Second, Executive Branch departments and agencies are subject to regulations that implement their authorizing statutes and to regulations imposed by other agencies, such as the Office of Management and Budget and the Office of Personnel Management. The House is subject to specific laws and its own rules and to regulations contained in its *Members' Congressional Handbook and Committees' Congressional Handbook*.

The sole, official purpose of this report is for informational use by Members of the U.S. House of Representatives, Office of the Chief Administrative Officer, and Office of Inspector General. It is not intended to be, and should not be, used by anyone other than these specified parties in an official capacity.

COTTON & COMPANY LLP

A handwritten signature in dark ink, appearing to read "Matthew H. Johnson".

Matthew H. Johnson, CPA  
Partner

April 30, 2007  
Alexandria, Virginia

This Page Intentionally Left Blank



# **Independent Auditor's Report on Internal Control**

This Page Intentionally Left Blank



Cotton & Company LLP  
635 Slaters Lane  
4<sup>th</sup> Floor  
Alexandria, VA 22314

P: 703.836.6701  
F: 703.836.0941  
www.cottoncpa.com

## INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL

To the Inspector General  
U.S. House of Representatives

Cotton & Company LLP has examined management's assertion included in the accompanying House of Representatives (House) Management Report on Internal Control. In that report, management asserted that the U.S. House of Representatives maintained effective internal control over financial reporting as of September 30, 2006, based on the *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. Management is responsible for maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on management's assertion based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and *Government Auditing Standards*, issued by the Comptroller General of the United States, and, accordingly, obtained an understanding of internal control over financial reporting; tested and evaluated design and operating effectiveness of internal control; and performed such other procedures as considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of internal control over financial reporting to future periods are subject to the risk that internal control may become inadequate as the result of changes in conditions, or that the degree of compliance with policies or procedures may deteriorate.

In our opinion, management's assertion that the U.S. House of Representatives maintained effective internal control over financial reporting as of September 30, 2006, is fairly stated, in all material respects, based upon *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States.

We did note certain matters involving internal control and its operations that we consider reportable conditions under standards issued by AICPA. Reportable conditions are matters coming to our attention related to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the House's ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements. These conditions are:

1. Weaknesses in the financial information system reduced the integrity of financial data and reporting.
2. Procedures used to ensure the completeness and accuracy of estimates, accruals, and other adjustments included in year-end financial statements were inadequate.

Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in an amount that would be material in relation to the financial statement being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We consider neither of these reportable conditions to be a material weakness. Additional details on the reportable conditions shown above are attached to this report.

The sole, official purpose of this report is for informational use by Members of the U.S. House of Representatives, Office of the Chief Administrative Officer, and Office of Inspector General. It is not intended to be, and should not be, used by anyone other than these specified parties in an official capacity. This report is, however, available to the public for informational purposes only.

COTTON & COMPANY LLP



Matthew H. Johnson, CPA, CISA, CGFM  
Partner

April 30, 2007  
Alexandria, Virginia

**STATUS OF INTERNAL CONTROL WEAKNESSES**  
**FISCAL YEAR 2006 FINANCIAL STATEMENT AUDIT**

Cotton & Company LLP assessed the status of weaknesses identified in the Calendar Year (CY) 2005 Independent Auditor's Report on Internal Control. The reportable conditions noted in CY 2005 continue to exist and are discussed in this report.

Our criteria for assessing control weaknesses are provided below along with a summary status of control weaknesses and detailed descriptions of these weaknesses.

**CRITERIA**

In determining the status of control weaknesses, we applied the following criteria:

- New Condition**      Newly identified weakness.
- Open (Prior Year)**      The House did not fully implement recommended corrective actions, or changes in House operations have not remedied or eliminated the need for recommended corrective action.
- Closed (Prior Year)**      The House fully implemented recommended corrective actions, or changes in House operations remedied or eliminated the need for recommended corrective action.

**SUMMARY STATUS OF INTERNAL CONTROL WEAKNESSES**

The following matrix provides a summary of new and existing internal control weaknesses:

<b>Weakness</b>	<b>Status as of April 30, 2007</b>		
	<b>New Condition</b>	<b>Open</b>	<b>Closed</b>
1. Weaknesses in the financial information system reduced the integrity of financial data and reporting. <i>(Reportable Condition)</i>		<b>X</b>	
2. Procedures used to ensure the completeness and accuracy of estimates, accruals, and other adjustments included in year-end financial statements were inadequate. <i>(Reportable Condition)</i>		<b>X</b>	

**DISCUSSION OF INTERNAL CONTROL WEAKNESSES****Weakness 1: Weaknesses in the financial information system reduced the integrity of financial data and reporting.**

**Summary Status:**      **Reportable Condition**  
                                 **Prior Condition**  
                                 **Open**

As part of the Fiscal Year (FY) 2006 financial statement audit, we reviewed physical, logical, and management controls over Office of the Chief Administrative Officer (CAO) information systems that process and report information on the annual financial statements. We reviewed controls used to secure and safeguard financial information traveling over the CAO network and residing on House financial systems. Our audit was limited to the CAO portion of the House network (general support system) and related financial information systems.

We relied upon government best practices developed by the National Institute of Standards and Technology (NIST) for review criteria. NIST was mandated by the Office of Management and Budget (OMB) to develop information technology (IT) audit tests, standards, and procedures to protect sensitive information from unauthorized access or modification for the federal government.

NIST guidance is accepted as industry best practice for establishing standards and procedures for securing information technology systems and protecting the integrity, confidentiality, reliability, and availability of information. NIST security guidance focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support.

In conducting our review, we examined internal controls over IT for the general support system and individual financial applications using the *Federal Information System Controls Audit Manual* (FISCAM), an accepted IT audit methodology developed by the Government Accountability Office (GAO). We examined controls in the following six areas:

- ? **Entity-wide security program planning and management controls** provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.
- ? **Access controls** limit or detect access to computer resources (data, program, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.
- ? **System software controls** limit and monitor access to powerful programs and sensitive files that control computer hardware and secure applications supported by the system.
- ? **Service continuity controls** ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected from destruction.

- ? **Application software development and program change controls** prevent implementation of unauthorized programs or modifications to existing programs.
- ? **Segregation-of-duty controls** provide policies, procedures, and organizational structure to prevent one individual from controlling key aspects of computer-related operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records. These controls must be applied within an application and at the mainframe and network system level.

Our system audits are performed on a multi-year rotational basis. We conduct a full review of one or more systems each year to ensure that during the audit cycle all system controls are adequately assessed. The FY 2006 audit included a systems internal control review of the Fixed Asset and Inventory Management System (FAIMS) and CAO entity-wide management controls. We also reviewed prior-year findings and recommendations to determine if management had taken action to correct identified weaknesses. We only tested those prior year recommendations where the CAO indicated that the corrective actions had been completed. Those recommendations that were tested are noted in the table.

Although CAO made some progress in addressing prior-year weaknesses, 31 of 37 prior-year recommendations remained open. Our audit also identified new weaknesses in three FISCAM control areas. Although none of the new or existing weaknesses discussed in this report by itself represents a reportable condition, they collectively comprise a reportable condition.

Weaknesses in each of the six FISCAM areas are discussed below.

### **Entity-Wide Security Program Planning and Management**

CAO's information system security program policies and procedures covering its network and financial applications need improvement. We identified the following entity-wide weakness during our FY 2006 audit:

#### **1. Corrective actions were not effectively implemented.**

Controls were not adequate to ensure that weaknesses identified in previous audits or reviews have been adequately addressed or corrected before being identified as closed by management. Specifically, the CAO did not have a process in place to effectively verify the effectiveness of actions taken to mitigate known weaknesses. During our financial statement audit, CAO management personnel stated that they considered actions to close 18 of the 37 prior-year findings and recommendations to have been appropriate. Based on management's assertion, we tested the 18 recommendations and determined that 12 had not been adequately addressed.

NIST Special Publication (SP) 800-55, *Security Metrics Guide for Information Technology Systems*, Section 5.5, Apply Corrective Actions, states:

*Phase 6 of the process, Apply Corrective Actions, involves implementing corrective actions in technical, management, and operational areas of security controls. After corrective actions are applied, the cycle completes itself and restarts with a subsequent data collection and analysis. Iterative data collection, analysis, and reporting will track progress of corrective actions, measure improvement, and identify*

*areas for further improvement. The iterative nature of the cycle ensures that the progress is monitored and the corrective actions are affecting system security control implementation in an intended way. Frequent performance measurements will ensure that if corrective actions are not implemented as planned, or if their effect is not as desired, quick course corrections can be made, internally to the organization, therefore avoiding problems being discovered during external audits, C&A efforts, or other similar activities.*

Without an effective process in place to ensure that control weaknesses have been adequately addressed, management cannot ensure that financial systems and the data they support are adequately protected.

While CAO has made improvements in this area, we recommend that the CAO:

New Recommendation	Recommendation Status	Management Response
1. Develop, document and implement a process for testing security controls identified as corrected, to ensure actions taken adequately mitigate or correct identified weaknesses.	New Recommendation	<b>CONCUR.</b> The CAO concurs with the recommendation to develop, document, and implement a process for testing controls identified as corrected. The CAO will implement this recommendation by October 31, 2007.

The following audit recommendations were made in past Office of the Inspector General (OIG) audit reports. Based on tests conducted during FY 2006, the underlying weakness of these recommendations still exists. To resolve them, we recommend that CAO continue to implement the partially resolved recommendations.

Prior Recommendations	Recommendation Status	Management Response
06-HOC-08, 1.01 Develop, document, and implement procedures to ensure all new CAO employees and contractors complete security awareness training before being granted access to the network and financial applications.	Open	<b>CONCUR.</b> The CAO concurs with the recommendation to ensure that all new CAO employees and contractors complete security awareness training. Security awareness training is offered online and once each month at the House Learning Center. All new CAO employees are notified that they must complete security awareness training within 30 days of their start date. The CAO believes we have taken all required action to close this part of the recommendation. The Information Systems Security Office and Human Capital will research solutions to the contractor security awareness training requirement and will present potential solutions by November 1, 2007.



Prior Recommendations	Recommendation Status	Management Response
<p>06-HOC-08, 1.02</p> <p>Develop, document, and implement a formal certification and accreditation program to achieve:</p> <ul style="list-style-type: none"> <li>? Certification and accreditation of general support system and all major financial applications.</li> <li>? Recertification every 3 years or when major changes occur.</li> <li>? Development of an SSP for the House general support system (network) to include requirements identified in HISPUB 024.</li> <li>? Identification of system owners and administrators including security administrators.</li> </ul> <p>Developing and fully implementing a formal certification and accreditation process should help resolve prior-year recommendations.</p>	Open	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to implement a formal certification and accreditation program. The Security Compliance Program has been documented in HISPOL 007.0, <i>Information Security Policy for the Information Security Compliance Program</i>. All CAO financial systems have completed the security certification process, including risk analyses, SSP in accordance with HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i> (formerly HISPUB 024 referenced above) which requires the identification of system owners and administrators, and risk assessments. The Compliance Program requires recertification every two years. The CAO believes we have taken all required action to close this part of the recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007. The baseline SSP for the House network will be completed by September 30, 2007.</p>
<p>06-HOC-08, 1.03</p> <p>Require all CAO employees and contractors users of the Network/Financial systems to read and sign expected rules of behavior annually as part of security awareness training. Signed statements should be retained for future use if necessary.</p>	Open	<p><b>CONCUR.</b></p> <p>CAO concurs with the recommendation to require CAO employees and contractors to read and sign expected rules of behavior. We will implement a variety of mechanisms to resolve this finding, as follows:</p> <ol style="list-style-type: none"> <li>1. All CAO staff are required to take annual security awareness training, which reviews acceptable use of House computer systems. The online training will be revised to explicitly identify expected rules of behavior, require the user to click to accept the rules of behavior before exiting the training, and record the user's acceptance. The CAO believes this electronic acceptance will satisfy the requirement to obtain signed forms. Printed copies of the rules of behavior will be provided to the House Learning Center for distribution to CAO staff and contractors who elect to attend the monthly security awareness seminar.</li> </ol>

Prior Recommendations	Recommendation Status	Management Response
		<ol style="list-style-type: none"> <li>1. Regarding users of financial applications, systems owners are required by HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i>, to obtain signed rules of behavior as part of the system access request process.</li> <li>2. Regarding network account holders, the CAO will explore ways to resolve this issue. Options under consideration include modifying future purchase orders and contracts to include the requirement for contractors to sign rules of behavior, coordinating with the Enterprise Technology Branch to obtain signed rules of behavior as part of the network account creation process, and working with Human Capital to obtain signed rules of behavior for new CAO staff and contractors as part of the on-boarding process.</li> </ol> <p>The CAO will complete these actions by December 31, 2007. We believe that, once implemented, these actions will close this recommendation.</p>
<p>03-HOC-05 3.02</p> <p>Establish a compliance program that would monitor and report on CAO business units' compliance with HISPOL and CAO policies for implementing computer security controls at the financial-application level.</p>	<p>Open Tested</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to establish a compliance program. The Compliance Program has been fully implemented in accordance with HISPOL 007.0, <i>Information Security Policy for the Information Security Compliance Program</i>. All CAO financial systems have completed the security certification process, including risk analyses, SSPs in accordance with HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i>, and risk assessments. The CAO believes we have taken all required actions to close this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.</p>
<p>04-HOC-07, 2.02</p> <p>Develop, document, and put in place procedures to ensure compliance with HISPOL 003.0. These procedures should include risk assessments performed at all levels (application, database, and server)</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to develop, document, and implement procedures to ensure compliance with HISPOL 003. These procedures are documented in HISPOL 007.0, <i>Information</i></p>

Prior Recommendations	Recommendation Status	Management Response
before new systems are installed and when enhancements are made to existing systems. In addition, this would include developing a schedule of risk assessments for existing and new financial systems and developing procedures to identify, implement, and track corrective actions designed to resolve weaknesses identified in the risk assessment.		<i>Security Policy for the Information Security Compliance Program.</i> All CAO financial systems have completed the security certification process, including risk analyses, SSPs in accordance with HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i> , and risk assessments. The financial systems will be reviewed and recertified every two years. Any weaknesses identified during the review are tracked to ensure that they are resolved within the agreed-upon timeframe. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.
04-HOC-07, 2.03  Develop procedures to ensure that system-specific security plans are developed and updated as needed to reflect changes to software, hardware, and business operations.	Open	<b>CONCUR.</b>  The CAO concurs with the recommendation regarding system-specific security plans. The SSPs for all CAO financial applications have been developed in accordance with HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i> . The SSPs will be reviewed annually and updated by the system owners to reflect changes to the respective system. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.
05-HOC-07, 2.02  Modify HISPUB 024 (pending) to require CAO SSPs to identify specific individuals as system and data owners.	Open	<b>CONCUR.</b>  The CAO concurs with the recommendation regarding the SSP guidance. HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i> , (formerly HIPSUB 024 referenced above) has been revised to identify system and data owners. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.
05-HOC-07, 2.03  Modify HISPUB 024 to include guidance on expected behaviors that should be documented within CAO SSPs. CAO should fully implement all requirements	Open	<b>CONCUR.</b>  The CAO concurs with the recommendation regarding the SSP guidance. HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i> , (formerly HIPSUB 024 referenced above) has been revised to

Prior Recommendations	Recommendation Status	Management Response
identified in HISPUB 024 by updating CAO SSPs to comply with HISPUB 024.		include guidance on expected behaviors. All SSPs for CAO financial applications have been updated accordingly. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

### **Access Controls**

Access controls over CAO major applications and the general support system were inadequate. We identified the following new weaknesses:

#### **1. Controls over FAIMS account administration were inadequate.**

Controls over administration of FAIMS accounts were inadequate. We selected a random sample of 45 FAIMS user accounts for testing and identified the following account administration weaknesses:

- ? Two user accounts tested had not been disabled or deleted after the supervisor stated the accounts were no longer needed during the semi-annual FAIMS account review process.
- ? Four user accounts tested had different FAIMS access than approved on access authorization forms.

NIST SP 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*, states the following:

Section 3.5.2 under User Administration:

*Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access.*

Section 3.5.2 under User Account Management:

*Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.*

Section 3.11.1, Identification:

*An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former users.*

Further, NIST SP 800-14, Inactive User IDs, states:

*User IDs that are inactive on the system for a specific period of time (e.g., 3 months) should be disabled.*

Without effective FAIMS account administration controls, unauthorized access and alteration of FAIMS financial data could occur and would be recorded as normal authorized activity.

## **2. FAIMS password controls were weak.**

Controls were inadequate to ensure that strong passwords were enforced for the FAIMS Oracle application in compliance with House policy and industry best practices. The FAIMS application cannot enforce strong passwords in accordance with HISPOL 009.0, Section 2 *Policy Guideline*, which states:

*Passwords must contain a minimum of eight characters in length and the following:*

- ? A combination of upper and lower case characters (e.g., a-z, A-Z)
- ? A combination of numbers and special characters (e.g., 9, !\*%&\$, etc.)

While FAIMS enforced a password length of eight characters or more, it did not require passwords to include upper and lower case characters, numbers, and special characters. Also, administrators were not conducting periodic audits of user passwords to determine they complied with House policy.

While management personnel stated they are comfortable with this weakness due to other controls in place (IP filtering), they have not formally documented their acceptance of this risk in writing.

The use of weak passwords can increase the likelihood of unauthorized individuals gaining access to the application either by guessing user passwords or using brute-force password crackers.

## **3. Incident response team members did not have requisite knowledge, skills, and abilities.**

Controls were inadequate to ensure that personnel with incident response responsibilities have the necessary knowledge, skills, and abilities to respond to incidents. The FAIMS program manager, whose responsibilities include FAIMS security, had not received training in House incident response procedures (HISPOL 004.0 and HISPUB 004.1). In addition, HISPOL 004.0 and HISPUB 004.1 do not require that team members be trained on incident response procedures.

NIST SP 800-14, Section 3.7.2, Characteristics states:

*An incident handling capability should have the following characteristics:*

*Educated Constituency. Users need to know about, accept, and trust the incident handling capability or it will not be used. Through training and awareness programs, users can become knowledgeable about the existence of the capability and how to recognize and report incidents. Users trust in the value of the service will build with reliable performance.*

Without adequate incident response training, the risk increases that individuals responsible for identifying and responding to incidents may not identify incidents or respond in a timely manner. In addition, damages to key financial systems or data may be greater as the result of poor response.

We recommend that the CAO:

New Recommendations	Recommendation Status	Management Response
<p>2. Enforce FAIMS account review policies and procedures to ensure that inactive accounts are disabled when no longer needed. Ensure that user access within FAIMS agrees with access documented on access request forms.</p>	<p>New Recommendation</p>	<p><b>CONCUR.</b></p> <p>Two measures will be taken to comply with this recommendation:</p> <ol style="list-style-type: none"> <li>1. The FAIMS account review policies will be expanded to include Security Request Verification Procedures to ensure inactive accounts are disabled when no longer needed.</li> <li>2. The Assets and CAO Advanced Business Solutions (CABS) Directorates will reconcile the existing User Responsibility Matrix with the actual Access Authorization Forms to ensure that user access within FAIMS agrees with access documented on access request forms. The FAIMS Account Review Policies will be updated to use the reconciled User Responsibility Matrix as the baseline.</li> </ol> <p>The CAO believes we will take the appropriate action to close this recommendation by November 1, 2007.</p>
<p>3. Implement controls to enforce passwords that comply with House policy.</p>	<p>New Recommendation</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the intent of this recommendation, however due to technology limitations, will implement the necessary compensating controls to reduce the level of risk. The CAO has implemented the following controls to mitigate this risk:</p> <ol style="list-style-type: none"> <li>1. FAIMS has implemented a complete set of controls on operating system passwords and database passwords in compliance with House policy.</li> <li>2. FAIMS has implemented all available controls on FAIMS Application passwords including:               <ol style="list-style-type: none"> <li>a. Minimum password length of 8 characters</li> <li>b. Password expiration after 60 days.</li> </ol> </li> </ol>

New Recommendations	Recommendation Status	Management Response
		<p>a. FAIMS DBAs monitor for multiple failed login attempts, on a weekly basis</p> <p>b. Users are knocked off the system after three failed login attempts, but the account is not disabled</p> <p>3. FAIMS has implemented IP Filtering: Users must connect to FAIMS from a PC which is included in the IP Filter list. By restricting access to FAIMS to users logged onto a distinct list of PCs, FAIMS is able to leverage the password complexity enforcement of Active Directory.</p> <p>CAO Management accepts this level of Risk and has compensating controls in place. To the extent feasible, the CAO believes we have taken the appropriate action to close this recommendation.</p>
4. Update House incident response policies to require annual incident response training and conduct annual training.	New Recommendation	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to update incident response policy to require annual incident response training and to conduct annual training. House Information Security Policy (HISPOL) 004.0, <i>Security Policy for Information Security Incidents</i>, will be updated to include annual incident response training. Initial training for the owners of the CAO financial systems will be completed by August 31, 2007. Annual refresher training will coincide with the yearly review of the System Security Plans (SSP.)</p>

The following audit recommendations were made in prior OIG audit reports. Based on tests conducted during FY 2006, the underlying weaknesses of these recommendations still exist. To resolve them, we recommend that the CAO continue to implement partially resolved recommendations.

Prior Recommendations	Recommendation Status	Management Response
<p>06-HOC-08, 1.04</p> <p>1. Develop procedures to ensure that access request forms are used for granting access to Paylinks in accordance with procedures documented in the Paylinks SSP.</p>	Open Tested	<p><b>CONCUR.</b></p> <p>1. The revised Standard Operating Procedure (SOP) will be completed and inserted into the PayLinks SSP by July 31, 2007.</p>

<b>Prior Recommendations</b>	<b>Recommendation Status</b>	<b>Management Response</b>
<ol style="list-style-type: none"> <li>2. Complete user access request forms for all individuals in Paylinks who do not have such forms. Access request forms should document the access level each user has been authorized.</li> <li>3. Update the Paylinks user access request form to include a space for the requesting supervisor and security administrator to sign and clearly show the Paylinks access level the user has been authorized.</li> </ol>		<ol style="list-style-type: none"> <li>2. The PayLinks user access forms that document the access level each user has been authorized for have been completed. The revised SOP will be completed and inserted into the PayLinks SSP. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.</li> <li>3. The PayLinks user access request form has been updated to include a space for the requesting supervisor and security administrator to sign and clearly show the PayLinks access level the user has been authorized for. The revised SOP will be completed and inserted into the PayLinks SSP. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007</li> </ol>
<p>06-HOC-08, 1.05</p> <p>Develop, document, and implement policies and procedures to ensure that Paylinks accounts are periodically reviewed and disabled or deleted when no longer needed.</p>	<p>Open Tested</p>	<p><b>CONCUR.</b></p> <p>The PayLinks SSP Section 10.5.3 describes the process for removing PayLinks accounts for users no longer employed by the House. PayLinks SSP Section 10.5.4 describes the process for quarterly review of all user accounts. The supporting documentation is currently under internal review and will be completed by July 31, 2007.</p>
<p>06-HOC-08, 1.07</p> <ol style="list-style-type: none"> <li>1. Develop policies and procedures to ensure that standard security configuration base lines are developed, tested, and implemented for all CAO financial applications before placing them into production.</li> <li>2. When management must configure a database against industry best practice for functionality reasons, clearly document this in the security baseline.</li> </ol>	<p>Open</p>	<p><b>CONCUR.</b></p> <ol style="list-style-type: none"> <li>1. The SSP template will be updated by HIR Information Security to reflect the policy and procedures to ensure that standard security configuration base lines are developed, tested, and implemented for all CAO financial applications. Additionally, the respective CAO financial applications will update their SSPs to incorporate the policy and procedures as defined in the SSP template. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.</li> <li>2. As part of the Information Security audit process, exceptions to the database checklists are noted as an</li> </ol>



Prior Recommendations	Recommendation Status	Management Response
		exception and must be mitigated, corrected, or risk accepted. The CAO believes we have taken the appropriate action to close this recommendation.
<p>06-HOC-08, 1.08</p> <p>Update Paylinks SSP to address logging and monitoring at the application and database levels. The SSP should identify what information or activities are to be logged, the length of time logs are to be retained, who has access to logs, and who should review logs.</p>	<p>Open Tested</p>	<p><b>CONCUR.</b></p> <p>The updated system logging is described in PayLinks SSP Section 10.4. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.</p>
<p>05-HOC-07, 2.04</p> <p>Take steps to ensure that all CAO network access requests are documented and retained for future reference.</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to document and retain all CAO network access requests. House Information Resources has implemented standard operating procedures to ensure that network access requests are validated, documented, and retained. These procedures have been approved and effective since May 21, 2007. The CAO believes this action is appropriate to close this recommendation.</p>
<p>05-HOC-07, 2.05</p> <p>Modify existing procedures to ensure that CAO system administrators are notified immediately when employees leave or are terminated from House employment. Assign responsibility for quarterly review of all CAO network accounts and require all reviews be documented for future reference. Reviewers should look for active accounts that have not been used in a specified period of time. Follow-up procedures should be performed to determine if they are still necessary and disabled and deleted if not.</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation regarding notification of terminated CAO employees. All CAO system owners and administrators are notified immediately when employees leave or are terminated from House employment. The CAO user account manager notifies system owners and administrators to conduct a quarterly review of the accounts under their purview. These procedures are documented in the <i>CAO Policy for User Account Management</i>, which was approved by the CAO on September 26, 2005. The CAO has also established additional internal quality control processes to ensure compliance with the policy. The CAO believes we have taken all required actions to close this recommendation.</p>
<p>05-HOC-07, 2.06</p> <p>Identify and document specific activities that security administrators should be logging and reviewing on a weekly basis, such as failed logon attempts, changes to</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with this recommendation. HISPUB 007.2.1, <i>System Security Plan Template for Major Applications</i>, requires system owners to log</p>

Independent Auditor's Report on Internal Control

Prior Recommendations	Recommendation Status	Management Response
		successful user logon and logoff, failed user logon attempts, password changes, account lockouts, and changes in user access permissions. System owners are required to review failed logon attempts weekly. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.
05-HOC-07, 2.09  Document policies and procedures for granting emergency and temporary access. Monitor emergency and temporary access and automatically terminate access after a predetermined period when possible.	Open	<b>CONCUR.</b>  The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007. CABS staff will work with the Finance directorate and CAO management to establish adequate criteria for granting emergency and temporary access, and systematic controls for termination of access after a predetermined period when possible.

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

06-HOC-08, 1.06  Take steps to ensure logon warning banners are in place and operating effectively for all CAO network users.
05-HOC-07, 2.08  Develop and implement policies and procedures to ensure that CAO system administrators are notified and access is removed on the same day an employee leaves or is terminated from the House.
05-HOC-07, 2.07  Finalize and implement HISPUB 022.0, Computer Security Incident Management. Effective implementation would include taking steps to ensure that all CAO system administrators are aware of the HISPUB and fully understand their roles and responsibilities for identifying and reporting potential security incidents.

**Systems Software Controls**

The following audit recommendations were made in prior-year OIG audit reports. Based on tests conducted during FY 2006, underlying weaknesses of these recommendations still exist. To resolve them, we recommend that CAO continue to implement these recommendations.

Prior Recommendations	Recommendation Status	Management Response
06-HOC-08, 1.09 Ensure that security audits are performed in accordance with House Information Security Policy 007.	Open	<b>CONCUR.</b>  The CAO concurs with the recommendation to ensure that security audits are performed

Prior Recommendations	Recommendation Status	Management Response
		<p>in accordance with H ISPO L 007.00, <i>Information Security Policy for the Information Security Compliance Program</i>. The Compliance Program has been fully implemented in accordance with H ISPO L 007.00, <i>Information Security Policy for the Information Security Compliance Program</i>. All CAO financial systems have completed security audits of servers, applications, and databases, and have been granted the appropriate level of security certification. The CAO believes we have taken all required actions to close this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.</p>
<p>06-HOC-08, 1.10</p> <p>Develop and document standard security configuration baselines for all operating systems supporting CAO financial applications to show how the operating system is intended to be configured. When risky or sensitive settings or processes must be used, management should clearly document reasons in the standard security configuration baseline.</p>	Open	<p><b>CONCUR.</b></p> <p>The CAO concurs with the recommendation to develop and document standard security configuration baselines for all operating systems supporting CAO financial applications. The CAO will implement this by September 30, 2007. Security configuration baselines, in the form of completed security checklist, have been completed for all operating systems supporting CAO financial applications. To support proper management and documentation of changes to the unique configuration of each financial system, the Enterprise Technology Branch is currently in the process of formalizing a new workflow. This new workflow will help ensure compliance at all times with Information Security audits of all systems. The workflow will address the unique security configuration for each financial system, documenting each system's unique evolution from the original HIR Security OS configuration checklist (baseline) to its current operational status. We expect this workflow to be formalized through the Technology Advisory Board by September 30, 2007. The CAO believes we will take the appropriate action to close this recommendation by an estimated completion date of October 31, 2007.</p>

The following prior-year recommendation was closed when changes in House operations remedied the associated underlying weaknesses:

## 05-HOC-07, 2.10

Modify existing HISPUBs and develop additional policies and procedures where necessary to ensure that all blank or default passwords are identified and changed before any CAO financial system is placed into production. Include specific steps in House audit checklists for determining if blank or default passwords exist.

**Service Continuity**

The following audit recommendations were made in a prior-year OIG audit report. Based on tests conducted during FY 2006, the underlying weaknesses of these recommendations still exist. To resolve them, we recommend that the CAO

<b>Prior Recommendations</b>	<b>Recommendation Status</b>	<b>Management Response</b>
06-HOC-08, 1.11  Develop, document, and test emergency procedures for the Ford data center. Ensure that procedures include specific steps to take during an emergency and identify who is responsible for taking such steps. Address activities such as emergency shutdown of systems and responding to fires or water leaks.	Open	<b>CONCUR.</b>  The CAO concurs with this recommendation. The ability to develop, document and test such procedures requires a fully functional and commissioned operating environment. While this documentation could be created before hand, it would at best be conjecture as to how the systems, alarms and other functional monitoring shall work. These systems are slated for commissioning in late 2007 as per the construction schedule. Emergency procedures shall be documented prior to completion of system commissioning and fully tested as part of the commissioning process. The CAO believes we will take the appropriate action to close this recommendation by December 31, 2007.
02-HOC-06, 4.5  Coordinate contingency planning and recovery policies and procedures to ensure a comprehensive approach that includes the network, mainframe computer, FFS, PD, and all critical financial systems.	Open	<b>CONCUR.</b>  The CAO concurs with this recommendation. Currently, the House maintains two distinct procedural documents in the support of contingency and recovery procedures for all systems. The first document addresses SOP related to the activation of Site 3, such as network, security, systems and support services. The second document provides greater detail on a system by system basis, to include emergency activation, system initiation steps and other support criteria for all systems. The SOP is currently under semi-annual review and is slated for approval and publication by July 31, 2007. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.

**Application Software Development and Program Change Control**

The following audit recommendations were made in a prior-year OIG audit report. Based on tests conducted during FY 2006, the underlying weaknesses of these recommendations still exist. To resolve them, we recommend that the CAO continue to implement partially resolved recommendations.

<b>Prior Recommendations</b>	<b>Recommendation Status</b>	<b>Management Response</b>
06-HOC-08, 1.12 Require that functional/technical specification documentation submitted by the developer be attached or included with change request forms and other documentation supporting changes to Paylinks.	Open Tested	<b>CONCUR.</b> The CAO partially concurs with this recommendation. The PayLinks team developed a Change Request form for internal change controls for software maintenance (SOP) that warrants no technical/functional specification documentation. For external changes involving software custom code changes (SOP), the Engineering Request (ER) form will be utilized. The ER form requires supporting Technical/Functional specification documentation be submitted. This ER form is sent to the TAB as an advisory notification. The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.
06-HOC-08, 1.13 Develop procedures to ensure that test plans and results for changes are documented and included with other documentation supporting changes to Paylinks.	Open Tested	<b>CONCUR.</b> External Change SOPs have been updated to reference test plan and results. The Internal Change SOP will reference what unit testing was completed, how, and results. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.
06-HOC-08, 1.15 Develop, document, and implement controls to ensure that only authorized and approved changes to Paylinks are introduced into production.	Open Tested	<b>CONCUR.</b> The process has been further refined. PayLinks changes are approved by the system owner via the Change Request form. The move of the change to production is authorized via the same Change Request form and procedures followed in the PayLinks Change SOPs. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.

Prior Recommendations	Recommendation Status	Management Response
06-HOC-08, 1.16 Periodically review production program changes to ensure that access and change controls are being followed.	Open	<b>CONCUR.</b> Please reference (06-HOC-08, 1.15). The PayLinks system owner will conduct an annual review of the production program changes to ensure that access and change controls are being followed. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.
06-HOC-08, 1.17 Develop, document, and implement controls over movement of program changes for Paylinks. Controls should be adequate to ensure that only authorized changes are moved into production, and management is notified.	Open Tested	<b>CONCUR.</b> Please reference (06-HOC-08, 1.15). The revised PayLinks Change SOPs reflect the necessary controls over the movement of program changes. With this process, only approved changes will be moved into production with proper notification to management. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.
06-HOC-08, 1.18 Develop and implement procedures to ensure that systems are developed and tested in accordance with House SDLC requirements and industry best practices, particularly in light of the forthcoming FFS replacement.	Open Tested	<b>CONCUR.</b> The CAO projects continue to adhere to SDLC policy and practices. Regarding ATLAS specifically, the project has made significant progress in moving through its life cycle. Several corresponding documents have been delivered and accepted. After the ATLAS Phase I lifecycle documentation is complete we will request closure of this item with an estimated completion date of November 30, 2007.

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

06-HOC-08, 1.14 Develop and document detailed test plan standards that define responsibilities for all personnel (users, programmers, quality assurance), require all test plans be approved, and require test results be documented and approved.
06-HOC-08, 1.19 Continue to address and resolve existing issues resulting from processing errors that occurred in Paylinks.

**Segregation-of-Duty Controls****5. Segregation-of-duty controls were inadequate.**

Controls were inadequate to ensure that FAIMS users did not have excessive access or the ability to perform incompatible functions.

NIST SP 800-14, Section 3.5.1, Staffing, states:

*Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.*

*Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database.*

Management had not implemented adequate segregation-of-duty controls as follows:

- We identified five database administrators who also have system administrator access in FAIMS. Allowing administrative access at both the database and application levels increases the likelihood of unauthorized activities occurring without management knowledge.
- The FAIMS system security officer (identified in the SSP) had administrative access within the application. NIST and industry best practice state that security personnel should not have high-level or administrative access in the systems they are responsible for auditing. For example, NIST SP 800-14, Section 3.13.2, Audit Trail Security Separation of Duties, states:

*Organizations should strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail.*

- One individual with system development responsibilities in FAIMS had system administrator access within the application. In addition, this access was not administered in accordance with the FAIMS SSP, which states:

*Developers do not have update privileges on the FAIMS production environment. If update privileges are required, the FAIMS Security Officer will review requests and grant permission to the production environment. The FAIMS Security Officer will then monitor activity and disable access upon completion of needed task.*

The risk of unauthorized or malicious code being introduced into the production environment is increased when developers are granted application access.

We recommend that the CAO:

New Recommendation	Recommendation Status	Management Response
<p>5. Identify, document, and implement controls for incompatible functions in FAIMS. Specific activities which should be considered include system administration, security administration, and system development. If management determined individuals need access within the system which is traditionally considered excessive or incompatible, management should identify and implement compensating controls to reduce the risk of unauthorized activities occurring.</p>	<p>New Recommendation</p>	<p><b>CONCUR.</b></p> <p>The CAO concurs with the intent of this recommendation, however due to resource limitations, will implement the necessary compensating controls to reduce the level of risk. The CAO will implement the following controls by July 31, 2007 to mitigate this risk:</p> <ol style="list-style-type: none"> <li>1. The FAIMS application "System Administrator" responsibility will be revoked from the DBAs. This will restrict them from:               <ol style="list-style-type: none"> <li>a. Creating, modifying and disabling users</li> <li>b. Changing passwords</li> <li>c. Granting responsibilities to users</li> <li>d. Creating and modifying responsibilities</li> </ol> </li> <li>2. The CAO has updated the SSP to identify the correct Security Officer.</li> <li>3. The CAO does not have the resources to separate the activities of developer and Application DBA.</li> </ol> <p>CAO Management accepts this level of Risk and has compensating controls in place.</p>

The following audit recommendations were made in a prior-year OIG audit report. Based on tests conducted during FY 2006, the underlying weaknesses of these recommendations still exist. To resolve them, we recommend that the CAO continue to implement partially resolved recommendations.

Prior Recommendations	Recommendation Status	Management Response
<p>06-HOC-08, 1.20</p> <p>Develop, document, and implement policies and procedures to ensure that CAO financial systems identify incompatible duties, and enforce segregation-of-duty controls both at end-user and administrative levels.</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>An internal CABS policy was issued on March 30, 2007 to have segregation-of-duties procedures for CABS financial applications. The CAO believes we have taken the appropriate action to close this recommendation.</p>
<p>06-HOC-08, 1.21</p> <p>Develop and implement procedures to ensure that segregation-of-duty principles are understood by key personnel, such as</p>	<p>Open</p>	<p><b>CONCUR.</b></p> <p>CABS staff will build procedures based upon the CABS policy issued on March 30, 2007 to ensure key CABS personnel have a</p>



<b>Prior Recommendations</b>	<b>Recommendation Status</b>	<b>Management Response</b>
system and data owners and program managers.		complete and thorough understanding of the segregation-of-duty principles. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.
06-HOC-08, 1.22 Identify and document incompatible administrative and end-user duties in Paylinks.	Open Tested	<b>CONCUR.</b> Paylinks SSP Section 10.1.1 will be updated to address this recommendation. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.
06-HOC-08, 1.23 Assign users in Paylinks to appropriate security classes to enforce proper segregation-of-duty controls. Follow the concept of least privilege when assigning users to security classes. Provide users with only enough system access to perform their assigned roles or responsibilities.	Open Tested	<b>CONCUR.</b> New Security Profile Class Listing reflects the new Functional roles and responsibilities separation of duties. The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.
06-HOC-08, 1.24 Remove Paylinks database and operating system administrator's access to the Paylinks application. If removal is not possible, limit access to only what is necessary for business purposes. In addition, put compensating controls in place to monitor administrator activities in the application.	Open	<b>CONCUR.</b> The CAO concurs with this recommendation. We have two security roles, DBA and SYSADMIN to facilitate this requirement (e.g. DBA is limited to running a currency code report and currency code inquiries). The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.

**Weakness 2: Procedures used to ensure the completeness and accuracy of estimates, accruals, and other adjustments included in year-end financial statements were inadequate.****Summary Status: Reportable Condition**

**Prior Condition: Revised Recommendation to replace CY 2005 Reportable Condition (The Financial Reporting Internal Control Framework was Inadequate)**

We identified several instances in which the House system of internal control over financial reporting did not ensure accurate reporting of transactions and balances. Internal control procedures to ensure the completeness and accuracy of estimates, accruals, and other adjustments included in the financial statements were not effective or did not exist in all cases.

Best practices of the federal government contained in OMB Circular A-123, *Management's Responsibility for Internal Control*, state that:

*Management is responsible for developing and maintaining effective internal control. Effective internal control provides assurance that significant weaknesses in the design or operation of internal control, that could adversely affect the agency's ability to meet its objectives, would be prevented or detected in a timely manner.*

We identified several instances in which management failed to implement adequate internal control to ensure the accurate preparation and presentation of the House's financial statements. Individually, these issues are not material to the financial statements. Taken collectively, however, they represent a significant deficiency in the effectiveness of internal control over financial reporting:

- ? The analysis used to accrue accounts payable at year-end did not identify all significant accounts payable transactions. The Office of Finance and Procurement (OFP) analyzed transactions occurring 45 days after the fiscal year-end to determine if transactions related to goods or services provided during FY 2006. OFP did not identify the completion date for all relevant transactions. This resulted in \$703,595 not being properly accrued as accounts payable as of September 30, 2006.
- ? Procedures to ensure the completeness and accuracy of prepaid expenses were not effective due to data quality issues. OFP used period-of-performance dates, which are input into the Federal Financial System (FFS) during the procurement cycle, to identify potential prepaid expenses. Our testing identified two expense transactions totaling \$881,588 that should have been classified as prepaid expenses as of September 30, 2006.
- ? House management did not have policies and procedures in place to verify the accuracy of transactions and balances reported on its annual financial statements for the Congressional Use of Foreign Currency fund (Foreign Currency fund). The Foreign Currency fund is used to finance Congressional travel to overseas locations and is administered by the U.S. Department of State on behalf of the House. The State Department reports fund balance transactions to the U.S. Department of Treasury on a monthly basis. OFP used information provided by Treasury to record adjusting entries to reflect Foreign Currency fund activities on the year-end financial statements. It

did not have procedures in place to determine the accuracy of information reported by Treasury for the Foreign Currency fund. As of September 30, 2006, the Foreign Currency fund had expense transactions totaling \$9,214,623 and a remaining fund balance of \$26,918,332.

- ? The process used by OFP to track and reverse temporary adjusting entries was ineffective. During FY 2006, OPF did not reverse an adjusting entry recorded to prepare the FY 2005 financial statements, resulting in an overstatement to FY 2006 revenues of \$1,898,409.

We recommend that the CAO:

New Recommendations	Recommendation Status	Management Response
<p>1. Refine the current accounts payable accrual process by:</p> <ul style="list-style-type: none"> <li>? Reviewing transactions recorded in the subsequent period and validating the completion date for all relevant transactions.</li> <li>? Annually comparing accounts payable accruals to subsequent year cut-off errors to identify variances and refine the accounts payable accrual process as needed.</li> </ul>	New Recommendation	<p><b>CONCUR.</b></p> <p>The Office of Financial Solutions will refine the current accounts payable accrual process used in preparing the House's annual financial statements. As in previous years, relevant receiver documents posted during the first 45 days subsequent to the end of the fiscal year will be analyzed and cross referenced to payment documents to determine whether the period of performance associated with the transaction indicates it should be recorded as accounts payable. However, we will improve upon the current process by ensuring that any receiver document not tied to a payment transaction is thoroughly researched and tied to supporting documentation such as purchase orders or invoices to determine whether it should be recorded as accounts payable. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.</p>
<p>2. Perform a statistically valid review of period of performance date fields in FFS to determine if data are reliable for use in prepayment estimates. If error rates are high, and thus preclude use of FFS performance date fields, then perform necessary procedures to:</p> <ul style="list-style-type: none"> <li>? Correct data entry issues.</li> <li>? Develop an alternative process to prepare prepaid expense estimates until the performance date data can be relied upon.</li> </ul>	New Recommendation	<p><b>CONCUR.</b></p> <p>The Office of Financial Solutions will perform a statistically valid review of period of performance date fields prior to preparing the House's Fiscal Year 2007 Financial Statements to determine whether this data can be relied upon to analyze and record prepaid expenses. We believe that the errors uncovered during substantive testing referenced in the audit report were the result of inadvertent deletions of service dates on certain payment transactions and do not represent systemic problems in the compilation process. If error rates are determined to be high, the Office of Financial Solutions will develop an alternative process to prepare prepaid expense estimates until the performance date data can be relied upon. The CAO</p>

Independent Auditor's Report on Internal Control

New Recommendations	Recommendation Status	Management Response
		believes we will take the appropriate action to close this recommendation by January 31, 2008.
3. Develop and implement a process to reconcile Foreign Currency fund balances to internal documents (e.g. travel authorizations) and Treasury on a monthly basis.	New Recommendation	<b>CONCUR.</b>  The Office of Financial Solutions will develop and implement a process to reconcile Foreign Currency fund balances at Treasury to internal documents used at the Department of State, and travel authorization documents used at the House, where applicable. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.
4. Develop and implement procedures to: ? Identify all temporary adjusting entries. ? Ensure that all temporary adjusting entries are reversed in the subsequent fiscal year.	New Recommendation	<b>CONCUR.</b>  The Office of Financial Solutions will develop and implement procedures to ensure that all accrual adjusting entries posted to the financial statements are reversed in the subsequent fiscal year. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

The following audit recommendations were made in past OIG audit reports. Based on tests conducted during FY 2006, the underlying weakness of these recommendations still exists. To resolve them, we recommend that the CAO implement recommendations not yet started.

Prior Recommendation	Recommendation Status	Management Response
05-HOC-07, 3.1  Review and revise <i>Accounting Department Policy and Procedures</i> and <i>Accounting Department Annual Financial Statement Compilation Procedures</i> , including quality control procedures, to ensure that all functions are fully and completely documented.	Open	<b>CONCUR.</b>  The Accounting Department will review and revise its policies and procedures and financial statement compilation procedures as necessary to ensure that all functions are fully and completely documented. Accounting periodically updates all procedures related to both operations and financial statement preparation as various methodologies change. To address weaknesses discovered during the financial statement audit, our next revisions will emphasize quality control procedures, daily processes and methodology changes to certain financial statement line items. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

Based upon results of FY 2006 audit procedures, the magnitude of conditions related to following prior-year recommendations was downgraded to deficiencies, recommendation updated, or House operations remedied the associated underlying weaknesses. As a result, the following prior year recommendations are closed.

05-HOC-07, 1.3
Develop adequate controls to manage and account for annual and sick leave for applicable employees.
05-HOC-07, 1.2
Develop a proposal, for Committee on House Administration approval, which corrects the payroll inefficiency of preparing and processing supplemental payroll.
06-HOC-08, 2.1
Require OFP to perform a thorough analysis of its procedures for preparing the SCF to ensure that all FFS and subsidiary ledger data are included and properly classified in the SCF.
06-HOC-08, 2.2
Require OFP to identify and implement a process to ensure a thorough review of the subsequent period to capture all financial reporting data. Document these activities in OFP policies and procedures manual.
06-HOC-08, 2.3
Require all CAO personnel responsible for capitalized property procurement, monitoring, and reporting to attend training in generally accepted accounting principles for fixed assets.
Prepare a memorandum to non-CAO offices responsible for purchasing capitalized property instructing them of the House's fixed-asset policies and provide training, if necessary.
06-HOC-08, 2.4
Develop and implement a policy requiring timely updates to FAIMS for all capitalized property purchases and discontinue use of manual worksheets.
Require OFP to revise its policies and procedures to state that assets removed from service should not be depreciated.
06-HOC-08, 2.5
Allow OFP staff responsible for property and equipment monitoring and reporting be granted FAIMS user access privileges to adjust capital asset costs, as necessary.
06-HOC-08, 2.6
Work with the Committee on House Administration to amend its rules and require annual inventories of capitalized internal use software. Subject capitalized software to the same acquisition, monitoring, and disposal controls as all other capitalized property.
06-HOC-08, 2.7
Investigate the design of controls over (1) payroll data entry and other Human Resource processes and management review functions and (2) review the Over Speaker Pay Edit report process to determine where weaknesses exist so these processes may be modified to ensure that similar errors are detected and prevented in the future.

This Page Intentionally Left Blank

## **Management Comments**

This Page Intentionally Left Blank



## **Management Report on Internal Control**

This Page Intentionally Left Blank

## The U.S. House of Representatives Management Report on Internal Control

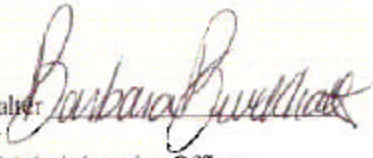
In connection with your examination of our assertion that the U.S. House of Representatives (House) maintained effective internal control over financial reporting as of September 30, 2006, for the purpose of expressing an opinion as to whether the assertion is fairly stated, in all material respects in accordance with standards prescribed by the Government Accountability Office in *Standards for Internal Control in the Federal Government*, dated November 1999, we confirm to the best of our knowledge and belief, the following representations made to you during your examination:

- We are responsible for establishing and maintaining effective internal control over financial reporting.
- We have performed an evaluation of the effectiveness of the House's internal control over financial reporting in accordance with standards prescribed by the General Accounting Office in *Standards for Internal Control in the Federal Government*, dated November 1999, the objectives of which include:
  - Effectiveness and efficiency of operations,
  - Reliability of financial reporting, and
  - Compliance with applicable laws and regulations.
- Based on our evaluation, we assert that the House maintained effective internal control over financial reporting as of September 30, 2006, based on the above-specified control criteria.
- We have disclosed to you all significant deficiencies in the design or operation of internal control that could adversely affect the House's ability to record, process, summarize, and report financial data consistent with our assertions in the financial statements.
- We have identified all deficiencies in internal control we believe to be material weaknesses.
- We have not encountered any instances of fraud by either:
  - Management or employees who have significant roles in internal control, or
  - Other employees that could have a material effect on the financial statements.
- Subsequent to the date of our management report, there have been no significant changes to internal control and no other factors have arisen that might significantly affect internal control, including any corrective action taken by the House with regard to significant deficiencies and material weaknesses.

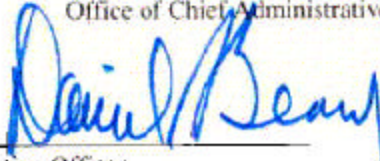
Kathy J. Perdue  
Assistant Chief Administrative Officer



Barbara Burkhalter  
Senior Advisor  
Office of Chief Administrative Officer



Daniel P. Beard  
Chief Administrative Officer



This Page Intentionally Left Blank

# **CAO Response to the 2006 Financial Statement Audit Report**

This Page Intentionally Left Blank

Office of the  
Chief Administrative Officer  
U.S. House of Representatives  
Washington, DC 20515-6860

MEMORANDUM

To: James Cornell  
Inspector General

From: Daniel P. Beard  
Chief Administrative Officer

Subject: CAO responses to *Independent Auditor's Report on Internal Control* related to the House of Representatives Fiscal Year 2006 Annual Financial Statement Audit

Date: JUN 07 2007

Thank you for the opportunity to comment on the subject audit report. We have carefully reviewed the report's findings and recommendations and concur with each of them.

The following is a brief response to each of the audit recommendations made in the audit report:

**Weakness 1:** Weaknesses in the financial information system reduced the integrity of financial data and reporting.

**Recommendation 1:** Develop, document, and implement a process for testing controls identified as corrected, to ensure actions taken adequately mitigate or correct identified weaknesses.

**CONCUR.**

The CAO concurs with the recommendation to develop, document, and implement a process for testing controls identified as corrected. The CAO will implement this recommendation by October 31, 2007.

**Recommendation 2:** Enforce Fixed Asset Inventory Management System (FAIMS) account review policies and procedures to ensure that inactive accounts are disabled when no longer needed. Ensure that user access within FAIMS agrees with access documented on access request forms.

**CONCUR.**

Two measures will be taken to comply with this recommendation:

1. The FAIMS account review policies will be expanded to include Security Request Verification Procedures to ensure inactive accounts are disabled when no longer needed.
2. The Assets and CAO Advanced Business Solutions (CABS) Directorates will reconcile the existing User Responsibility Matrix with the actual Access Authorization Forms to



ensure that user access within FAIMS agrees with access documented on access request forms. The FAIMS Account Review Policies will be updated to use the reconciled User Responsibility Matrix as the baseline.

The CAO believes we will take the appropriate action to close this recommendation by November 1, 2007.

**Recommendation 3:** Implement controls to enforce passwords that comply with House policy.

**CONCUR.**

The CAO concurs with the intent of this recommendation, however due to technology limitations, will implement the necessary compensating controls to reduce the level of risk. The CAO has implemented the following controls to mitigate this risk:

1. FAIMS has implemented a complete set of controls on operating system passwords and database passwords in compliance with House policy.
2. FAIMS has implemented all available controls on FAIMS Application passwords including:
  - a. Minimum password length of 8 characters
  - b. Password expiration after 60 days
  - c. FAIMS DBAs monitor for multiple failed login attempts, on a weekly basis
  - d. Users are knocked off the system after three failed login attempts, but the account is not disabled
3. FAIMS has implemented IP Filtering: Users must connect to FAIMS from a PC which is included in the IP Filter list. By restricting access to FAIMS to users logged onto a distinct list of PCs, FAIMS is able to leverage the password complexity enforcement of Active Directory.

CAO Management accepts this level of Risk and has compensating controls in place. To the extent feasible, the CAO believes we have taken the appropriate action to close this recommendation.

**Recommendation 4:** Update House incident response policies to require annual incident response training and conduct annual training.

**CONCUR.**

The CAO concurs with the recommendation to update incident response policy to require annual incident response training and to conduct annual training. House Information Security Policy (HISPOL) 004.0, *Security Policy for Information Security Incidents*, will be updated to include annual incident response training. Initial training for the owners of the CAO financial systems will be completed by August 31, 2007. Annual refresher training will coincide with the yearly review of the System Security Plans (SSP.)

**Recommendation 5:** Identify, document, and implement controls for incompatible functions in FAIMS. Specific activities which should be considered include system administration, security administration, and system development.



If management determined individuals need access within the system which is traditionally considered excessive or incompatible, management should identify and implement compensating controls to reduce the risk of unauthorized activities occurring.

**CONCUR.**

The CAO concurs with the intent of this recommendation, however due to resource limitations, will implement the necessary compensating controls to reduce the level of risk. The CAO will implement the following controls by July 31, 2007 to mitigate this risk:

1. The FAIMS application "System Administrator" responsibility will be revoked from the DBAs. This will restrict them from:
  - a. Creating, modifying and disabling users
  - b. Changing passwords
  - c. Granting responsibilities to users
  - d. Creating and modifying responsibilities
2. The CAO has updated the SSP to identify the correct Security Officer.
3. The CAO does not have the resources to separate the activities of developer and Application DBA.

CAO Management accepts this level of Risk and has compensating controls in place.

**STATUS OF PRIOR-YEAR RECOMMENDATIONS**

**Recommendation:** *(06-HOC-08, 1.01)* Develop, document, and implement procedures to ensure all new CAO employees and contractors complete security awareness training before being granted access to the network and financial applications.

**CONCUR.**

The CAO concurs with the recommendation to ensure that all new CAO employees and contractors complete security awareness training. Security awareness training is offered online and once each month at the House Learning Center. All new CAO employees are notified that they must complete security awareness training within 30 days of their start date. The CAO believes we have taken all required action to close this part of the recommendation. The Information Systems Security Office and Human Capital will research solutions to the contractor security awareness training requirement and will present potential solutions by November 1, 2007.

**Recommendation:** *(06-HOC-08, 1.02)* Develop, document, and implement a formal certification and accreditation program to achieve:

- Certification and accreditation of the general support system and all major financial applications.
- Recertification every 3 years or when major changes occur.

- Development of an SSP for the House general support system (network) to include requirements identified in House Information Security Publication (HISPUB) 024.
- Identification of system owners and administrators including security administrators.

Developing and fully implementing a formal certification and accreditation process should help resolve prior-year recommendations.

#### **CONCUR.**

The CAO concurs with the recommendation to implement a formal certification and accreditation program. The Security Compliance Program has been documented in HISPOL 007.0, *Information Security Policy for the Information Security Compliance Program*. All CAO financial systems have completed the security certification process, including risk analyses, SSP in accordance with HISPUB 007.2.1, *System Security Plan Template for Major Applications* (formerly HISPUB 024 referenced above) which requires the identification of system owners and administrators, and risk assessments. The Compliance Program requires recertification every two years. The CAO believes we have taken all required action to close this part of the recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007. The baseline SSP for the House network will be completed by September 30, 2007.

**Recommendation:** (06-HOC-08, 1.03) Require all CAO employees and contractors users of the Network/Financial systems to read and sign expected rules of behavior annually as part of security awareness training. Signed statements should be retained for future use if necessary.

#### **CONCUR.**

CAO concurs with the recommendation to require CAO employees and contractors to read and sign expected rules of behavior. We will implement a variety of mechanisms to resolve this finding, as follows:

1. All CAO staff are required to take annual security awareness training, which reviews acceptable use of House computer systems. The online training will be revised to explicitly identify expected rules of behavior, require the user to click to accept the rules of behavior before exiting the training, and record the user's acceptance. The CAO believes this electronic acceptance will satisfy the requirement to obtain signed forms. Printed copies of the rules of behavior will be provided to the House Learning Center for distribution to CAO staff and contractors who elect to attend the monthly security awareness seminar.
2. Regarding users of financial applications, systems owners are required by HISPUB 007.2.1, *System Security Plan Template for Major Applications*, to obtain signed rules of behavior as part of the system access request process.
3. Regarding network account holders, the CAO will explore ways to resolve this issue. Options under consideration include modifying future purchase orders and contracts to include the requirement for contractors to sign rules of behavior, coordinating with the



Enterprise Technology Branch to obtain signed rules of behavior as part of the network account creation process, and working with Human Capital to obtain signed rules of behavior for new CAO staff and contractors as part of the on-boarding process.

The CAO will complete these actions by December 31, 2007. We believe that, once implemented, these actions will close this recommendation.

**Recommendation:** (03-HOC-05, 3.02) Establish a compliance program that would monitor and report on CAO business units' compliance with HISPOL and CAO policies for implementing computer security controls at the financial application level.

**CONCUR.**

The CAO concurs with the recommendation to establish a compliance program. The Compliance Program has been fully implemented in accordance with HISPOL 007.0, *Information Security Policy for the Information Security Compliance Program*. All CAO financial systems have completed the security certification process, including risk analyses, SSPs in accordance with HISPUB 007.2.1, *System Security Plan Template for Major Applications*, and risk assessments. The CAO believes we have taken all required actions to close this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (04-HOC-07, 2.02) Develop, document, and put in place procedures to ensure compliance with HISPOL 003.0. These procedures should include risk assessments performed at all levels (application, database, and server) before new systems are installed and when enhancements are made to existing systems. In addition, this would include developing a schedule of risk assessments for existing and new financial systems and developing procedures to identify, implement, and track corrective actions designed to resolve weaknesses identified in the risk assessment.

**CONCUR.**

The CAO concurs with the recommendation to develop, document, and implement procedures to ensure compliance with HISPOL 003. These procedures are documented in HISPOL 007.0, *Information Security Policy for the Information Security Compliance Program*. All CAO financial systems have completed the security certification process, including risk analyses, SSPs in accordance with HISPUB 007.2.1, *System Security Plan Template for Major Applications*, and risk assessments. The financial systems will be reviewed and recertified every two years. Any weaknesses identified during the review are tracked to ensure that they are resolved within the agreed-upon timeframe. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (04-HOC-07, 2.03) Develop procedures to ensure that system-specific security plans are developed and updated as needed to reflect changes to software, hardware, and business operations.

**CONCUR.**

The CAO concurs with the recommendation regarding system-specific security plans. The SSPs for all CAO financial applications have been developed in accordance with HISPUB 007.2.1, *System Security Plan Template for Major Applications*. The SSPs will be reviewed annually and updated by the system owners to reflect changes to the respective system. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (05-HOC-07, 2.02) Modify HISPUB 024 (pending) to require CAO SSPs to identify specific individuals as system and data owners.

**CONCUR.**

The CAO concurs with the recommendation regarding the SSP guidance. HISPUB 007.2.1, *System Security Plan Template for Major Applications*, (formerly HIPSUB 024 referenced above) has been revised to identify system and data owners. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (05-HOC-07, 2.03) Modify HISPUB 024 to include guidance on expected behaviors that should be documented within CAO SSPs. CAO should fully implement all requirements identified in HISPUB 024 by updating CAO SSPs to comply with HISPUB 024.

**CONCUR.**

The CAO concurs with the recommendation regarding the SSP guidance. HISPUB 007.2.1, *System Security Plan Template for Major Applications*, (formerly HIPSUB 024 referenced above) has been revised to include guidance on expected behaviors. All SSPs for CAO financial applications have been updated accordingly. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (06-HOC-08, 1.04)

1. Develop procedures to ensure that access request forms are used for granting access to Paylinks in accordance with procedures documented in the Paylinks SSP.
2. Complete user access request forms for all individuals in Paylinks who do not have such forms. Access request forms should document the access level each user has been authorized.
3. Update the Paylinks user access request form to include a space for the requesting supervisor and security administrator to sign and clearly show the Paylinks access level the user has been authorized.



**CONCUR.**

1. The revised Standard Operating Procedure (SOP) will be completed and inserted into the PayLinks SSP by July 31, 2007.
2. The PayLinks user access forms that document the access level each user has been authorized for have been completed. The revised SOP will be completed and inserted into the PayLinks SSP. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.
3. The PayLinks user access request form has been updated to include a space for the requesting supervisor and security administrator to sign and clearly show the PayLinks access level the user has been authorized for. The revised SOP will be completed and inserted into the PayLinks SSP. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007

**Recommendation:** (06-HOC-08, 1.05) Develop, document, and implement policies and procedures to ensure that Paylinks accounts are periodically reviewed and disabled or deleted when no longer needed.

**CONCUR.**

The PayLinks SSP Section 10.5.3 describes the process for removing PayLinks accounts for users no longer employed by the House. PayLinks SSP Section 10.5.4 describes the process for quarterly review of all user accounts. The supporting documentation is currently under internal review and will be completed by July 31, 2007.

**Recommendation:** (06-HOC-08, 1.07)

1. Develop policies and procedures to ensure that standard security configuration baselines are developed, tested, and implemented for all CAO financial applications before placing them into production.
2. When management must configure a database against industry best practice for functionality reasons, clearly document this in the security baseline.

**CONCUR.**

1. The SSP template will be updated by HIR Information Security to reflect the policy and procedures to ensure that standard security configuration baselines are developed, tested, and implemented for all CAO financial applications. Additionally, the respective CAO financial applications will update their SSPs to incorporate the policy and procedures as defined in the SSP template. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.
2. As part of the Information Security audit process, exceptions to the database checklists are noted as an exception and must be mitigated, corrected, or risk accepted. The CAO believes we have taken the appropriate action to close this recommendation.

**Recommendation:** (06-HOC-08, 1.08) Update Paylinks SSP to address logging and monitoring at the application and database levels. The SSP should identify what information or activities are to be logged, the length of

time logs are to be retained, who has access to logs, and who should review the logs.

**CONCUR.**

The updated system logging is described in PayLinks SSP Section 10.4. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.

**Recommendation:** (05-HOC-07, 2.04) Take steps to ensure that all CAO network access requests are documented and retained for future reference.

**CONCUR.**

The CAO concurs with the recommendation to document and retain all CAO network access requests. House Information Resources has implemented standard operating procedures to ensure that network access requests are validated, documented, and retained. These procedures have been approved and effective since May 21, 2007. The CAO believes this action is appropriate to close this recommendation.

**Recommendation:** (05-HOC-07, 2.05) Modify existing procedures to ensure that CAO system administrators are notified immediately when employees leave or are terminated from House employment. Assign responsibility for quarterly review of all CAO network accounts and require all reviews be documented for future reference. Reviewers should look for active accounts that have not been used in a specified period of time. Follow-up procedures should be performed to determine if they are still necessary and disabled or deleted if not.

**CONCUR.**

The CAO concurs with the recommendation regarding notification of terminated CAO employees. All CAO system owners and administrators are notified immediately when employees leave or are terminated from House employment. The CAO user account manager notifies system owners and administrators to conduct a quarterly review of the accounts under their purview. These procedures are documented in the *CAO Policy for User Account Management*, which was approved by the CAO on September 26, 2005. The CAO has also established additional internal quality control processes to ensure compliance with the policy. The CAO believes we have taken all required actions to close this recommendation.

**Recommendation:** (05-HOC-07, 2.06) Identify and document specific activities that security administrators should be logging and reviewing on a weekly basis such as failed logon attempts, changes to security profiles, and unsuccessful attempts to access unauthorized systems or data by users and outsiders.

**CONCUR.**

The CAO concurs with this recommendation. HISPUB 007.2.1, *System Security Plan Template for Major Applications*, requires system owners to log successful user logon and logoff, failed user logon attempts, password changes, account lockouts, and changes in user access



permissions. System owners are required to review failed logon attempts weekly. The CAO believes we have taken all actions necessary to complete this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (05-HOC-07, 2.09) Document policies and procedures for granting emergency and temporary access. Monitor emergency and temporary access, and automatically terminate access after a predetermined period when possible.

**CONCUR.**

The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007. CABS staff will work with the Finance directorate and CAO management to establish adequate criteria for granting emergency and temporary access, and systematic controls for termination of access after a predetermined period when possible.

**Recommendation:** (06-HOC-08, 1.09) Ensure that security audits are performed in accordance with HISPOL 007.00, *Information Security Policy for the Information Security Compliance Program*.

**CONCUR.**

The CAO concurs with the recommendation to ensure that security audits are performed in accordance with HISPOL 007.00, *Information Security Policy for the Information Security Compliance Program*. The Compliance Program has been fully implemented in accordance with HISPOL 007.00, *Information Security Policy for the Information Security Compliance Program*. All CAO financial systems have completed security audits of servers, applications, and databases, and have been granted the appropriate level of security certification. The CAO believes we have taken all required actions to close this recommendation. Supporting documentation is currently under internal review and will be completed by August 31, 2007.

**Recommendation:** (06-HOC-08, 1.10) Develop and document standard security configuration baselines for all operating systems supporting CAO financial applications to show how the operating system is intended to be configured. When risky or sensitive settings or processes must be used, management should clearly document reasons in the standard security configuration baseline.

**CONCUR.**

The CAO concurs with the recommendation to develop and document standard security configuration baselines for all operating systems supporting CAO financial applications. The CAO will implement this by September 30, 2007. Security configuration baselines, in the form of completed security checklist, have been completed for all operating systems supporting CAO financial applications. To support proper management and documentation of changes to the unique configuration of each financial system, the Enterprise Technology Branch is currently in the process of formalizing a new workflow. This new workflow will help ensure compliance at all times with Information Security audits of all systems. The workflow will address the unique security configuration for each financial system, documenting each system's

requires supporting Technical/Functional specification documentation be submitted. This ER form is sent to the TAB as an advisory notification. The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.

**Recommendation:** (06-HOC-08, 1.13) Develop procedures to ensure that test plans and results for changes are documented and included with other documentation supporting changes to Paylinks.

**CONCUR.**

External Change SOPs have been updated to reference test plan and results. The Internal Change SOP will reference what unit testing was completed, how, and results. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.

**Recommendation:** (06-HOC-08, 1.15) Develop, document, and implement controls to ensure that only authorized and approved changes to Paylinks are introduced into production.

**CONCUR.**

The process has been further refined. PayLinks changes are approved by the system owner via the Change Request form. The move of the change to production is authorized via the same Change Request form and procedures followed in the PayLinks Change SOPs. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.

**Recommendation:** (06-HOC-08, 1.16) Periodically review production program changes to ensure that access and change controls are being followed.

**CONCUR.**

Please reference (06-HOC-08, 1.15). The PayLinks system owner will conduct an annual review of the production program changes to ensure that access and change controls are being followed. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.

**Recommendation:** (06-HOC-08, 1.17) Develop, document, and implement controls over movement of program changes for Paylinks. Controls should be adequate to ensure that only authorized changes are moved into production, and management is notified.

**CONCUR.**

Please reference (06-HOC-08, 1.15). The revised PayLinks Change SOPs reflect the necessary controls over the movement of program changes. With this process, only approved changes will be moved into production with proper notification to management. The CAO believes we have taken the appropriate action to close this recommendation. Supporting documentation is currently under internal review and will be completed by July 31, 2007.



unique evolution from the original HIR Security OS configuration checklist (baseline) to its current operational status. We expect this workflow to be formalized through the Technology Advisory Board by September 30, 2007. The CAO believes we will take the appropriate action to close this recommendation by an estimated completion date of October 31, 2007.

**Recommendation:** (06-HOC-08, 1.11) Develop, document, and test emergency procedures for the Ford data center. Ensure that procedures include specific steps to take during an emergency and identify who is responsible for taking such steps. Address activities such as emergency shut down of systems and responding to fires or water leaks.

**CONCUR.**

The CAO concurs with this recommendation. The ability to develop, document and test such procedures requires a fully functional and commissioned operating environment. While this documentation could be created beforehand, it would at best be conjecture as to how the systems, alarms and other functional monitoring shall work. These systems are slated for commissioning in late 2007 as per the construction schedule. Emergency procedures shall be documented prior to completion of system commissioning and fully tested as part of the commissioning process. The CAO believes we will take the appropriate action to close this recommendation by December 31, 2007.

**Recommendation:** (02-HOC-06, 4.05) Coordinate contingency planning and recovery policies and procedures to ensure a comprehensive approach that includes the network, mainframe computer, Federal Financial System (FFS), Procurement Desktop, and all critical financial systems.

**CONCUR.**

The CAO concurs with this recommendation. Currently, the House maintains two distinct procedural documents in the support of contingency and recovery procedures for all systems. The first document addresses SOP related to the activation of Site 3, such as network, security, systems and support services. The second document provides greater detail on a system by system basis, to include emergency activation, system initiation steps and other support criteria for all systems. The SOP is currently under semi-annual review and is slated for approval and publication by July 31, 2007. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.

**Recommendation:** (06-HOC-08, 1.12) Require that functional/ technical specification ~~documentation submitted by the developer be attached or included with~~ change request forms and other documentation supporting changes to Paylinks.

**CONCUR.**

The CAO partially concurs with this recommendation. The PayLinks team developed a Change Request form for internal change controls for software maintenance (SOP) that warrants no technical/functional specification documentation. For external changes involving software custom code changes (SOP), the Engineering Request (ER) form will be utilized. The ER form

**Recommendation:** (06-HOC-08, 1.18) Develop and implement procedures to ensure that systems are developed and tested in accordance with House SDLC requirements and industry best practices, particularly in light of the forthcoming FFS replacement.

**CONCUR.**

The CAO projects continue to adhere to SDLC policy and practices. Regarding ATLAS specifically, the project has made significant progress in moving through its life cycle. Several corresponding documents have been delivered and accepted. After the ATLAS Phase I lifecycle documentation is complete we will request closure of this item with an estimated completion date of November 30, 2007.

**Recommendation:** (06-HOC-08, 1.20) Develop, document, and implement policies and procedures to ensure that CAO financial systems identify incompatible duties and enforce segregation-of-duty controls both at the end user and administrative levels.

**CONCUR.**

An internal CABS policy was issued on March 30, 2007 to have segregation-of-duties procedures for CABS financial applications. The CAO believes we have taken the appropriate action to close this recommendation.

**Recommendation:** (06-HOC-08, 1.21) Develop and implement procedures to ensure that segregation-of-duty principles are understood by key personnel, such as system and data owners and program managers.

**CONCUR.**

CABS staff will build procedures based upon the CABS policy issued on March 30, 2007 to ensure key CABS personnel have a complete and thorough understanding of the segregation-of-duty principles. The CAO believes we will take the appropriate action to close this recommendation by August 31, 2007.

**Recommendation:** (06-HOC-08, 1.22) Identify and document incompatible administrative and end-user duties in Paylinks.

**CONCUR.**

PayLinks SSP Section 10.1.1 will be updated to address this recommendation. The CAO believes we will take the appropriate action to close this recommendation by July 31, 2007.

**Recommendation:** (06-HOC-08, 1.23) Assign users in Paylinks to appropriate security classes to enforce proper segregation-of-duty controls. Follow the concept of least-privilege when assigning users to security classes. Provide users with only enough system access to perform their assigned roles or responsibilities.



**CONCUR.**

New Security Profile Class Listing reflects the new Functional roles and responsibilities separation of duties. The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.

**Recommendation:** (06-HOC-08, 1.24) Remove Paylinks database and operating system administrator's access to the Paylinks application. If removal is not possible, limit access to only what is necessary for business purposes. In addition, put compensating controls in place to monitor administrator activities in the application.

**CONCUR.**

The CAO concurs with this recommendation. We have two security roles, DBA and SYSADMIN to facilitate this requirement (e.g. DBA is limited to running a currency code report and currency code inquiries). The CAO believes we have taken the appropriate action to close this recommendation with an estimated completion date of July 31, 2007.

**Weakness 2:** Procedures used to ensure the completeness and accuracy of estimates, accruals, and other adjustments included in year-end financial statements were inadequate.

**Recommendation 1:** Refine the current accounts payable accrual process by:

- Reviewing transactions recorded in the subsequent period and validating the completion date for all relevant transactions.
- Annually comparing accounts payable accruals to subsequent year cut-off errors to identify variances and refine the accounts payable accrual process as needed.

**CONCUR.**

The Office of Financial Solutions will refine the current accounts payable accrual process used in preparing the House's annual financial statements. As in previous years, relevant receiver documents posted during the first 45 days subsequent to the end of the fiscal year will be analyzed and cross referenced to payment documents to determine whether the period of performance associated with the transaction indicates it should be recorded as accounts payable. However, we will improve upon the current process by ensuring that any receiver document not tied to a payment transaction is thoroughly researched and tied to supporting documentation such as purchase orders or invoices to determine whether it should be recorded as accounts payable. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

**Recommendation 2:** Perform a statistically valid review of period of performance date fields in FFS to determine if data are reliable for use in prepayment estimates. If error rates are high, and thus preclude use of FFS performance date fields, then perform necessary procedures to:

- Correct data entry issues.

- Develop an alternative process to prepare prepaid expense estimates until the performance date data can be relied upon.

**CONCUR.**

The Office of Financial Solutions will perform a statistically valid review of period of performance date fields prior to preparing the House's Fiscal Year 2007 Financial Statements to determine whether this data can be relied upon to analyze and record prepaid expenses. We believe that the errors uncovered during substantive testing referenced in the audit report were the result of inadvertent deletions of service dates on certain payment transactions and do not represent systemic problems in the compilation process. If error rates are determined to be high, the Office of Financial Solutions will develop an alternative process to prepare prepaid expense estimates until the performance date data can be relied upon. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

**Recommendation 3:** Develop and implement a process to reconcile Foreign Currency fund balances to internal documents (e.g. travel authorization) and Treasury on a monthly basis.

**CONCUR.**

The Office of Financial Solutions will develop and implement a process to reconcile Foreign Currency fund balances at Treasury to internal documents used at the Department of State, and travel authorization documents used at the House, where applicable. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

**Recommendation 4:** Develop and implement procedures to:

- Identify all temporary adjusting entries.
- Ensure that all temporary adjusting entries are reversed in the subsequent fiscal year.

**CONCUR.**

The Office of Financial Solutions will develop and implement procedures to ensure that all accrual adjusting entries posted to the financial statements are reversed in the subsequent fiscal year. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.

**Recommendation 5:** Develop and implement a procedure to monitor the in-service dates related to capital asset transactions recorded in FAIMS and determine if adjustments are needed to:

- House financial statements; and/or
- Processes used to record transactions in FAIMS in a timely manner.

**CONCUR.**

This recommendation was deleted.

## **STATUS OF PRIOR-YEAR RECOMMENDATIONS**

**Recommendation:** (05-HOC-07, 3.1) Review and revise *Accounting Department Policy and Procedures* and *Accounting Department Annual Financial Statement Compilation Procedures*, including quality control procedures, to ensure that all functions are fully and completely documented.

### **CONCUR.**

The Accounting Department will review and revise its policies and procedures and financial statement compilation procedures as necessary to ensure that all functions are fully and completely documented. Accounting periodically updates all procedures related to both operations and financial statement preparation as various methodologies change. To address weaknesses discovered during the financial statement audit, our next revisions will emphasize quality control procedures, daily processes and methodology changes to certain financial statement line items. The CAO believes we will take the appropriate action to close this recommendation by January 31, 2008.